账号风控平台

开发对接指南

产品文档

腾讯云

文档目录

开发对接指南

概述

最近更新时间：2023-12-22 11:42:07

本指南介绍应用系统接入 CIAM 的方法及相应的 API。通过对接 CIAM，您的应用可以快速实现用户的登录、退出、注册等功能，并集成 CIAM 灵活、强大的配置与管理能力。

应用类型

基于常见的业务场景，CIAM 将应用分为以下几种类型：

Web 应用

运行在后端 Web 服务器上的应用系统，一般采用 Java, .NET, PHP, Node.js, Express 等语言或框架开发，用户通过浏览器访问应用。由于后端程序一般在受保护的服务器上运行，Web 应用能较好地存储应用密码等敏感信息，并保护 Token 等动态信息不泄露。

单页应用 (SPA)

直接运行在浏览器中的前端应用程序，一般采用 HTML、CSS 和 JavaScript 技术结合 React、Vue 和 Angular 等框架开发。单页应用可以直接向业务面 API 发起请求而无需经过后端程序转发，但由于程序和数据都存在于 user-agent (如浏览器) 中，单页应用不适合存储或处理需要受保护的敏感信息。

移动 App

安装和运行在用户设备 (如手机、平板电脑、PC、智能设备) 上的应用程序，一般采用专门的应用开发语言开发，如 Objective-C、Swift、 Kotlin 等。此类应用不适合存储应用密码等敏感信息，但一般能够保护 Token 等动态信息不泄露。

M2M 应用 (Machine to Machine)

运行在后端的应用程序 (如后端服务、命令行程序、守护进程)，一般通过调用其他的 API 来实现业务功能，无需用户参与。此类应用能够较好地保护敏感信息不泄露。

接入概览

Web 应用、SPA 和 移动 App 可以作为 OIDC (OAuth) 标准客户端快速接入 CIAM。OIDC 和 OAuth 协议在互联网的应用十分广泛，其相应的开发资源也非常丰富，各类应用一般都能找到开发库快速完成接入。
M2M 应用一般使用 客户端凭证模式获取 Access Token 后，携带 Access Token 访问相应的 API。

注意：

本指南的 API 通过 HTTPS 协议访问，访问地址前缀是您的用户目录域名，可以在 域名设置页面 查看。在本指南中，使用 `https://sample.portal.tencentciam.com` 作为访问地址前缀。

使用认证 API 接入
用户注册

最近更新时间：2023-12-22 11:42:07

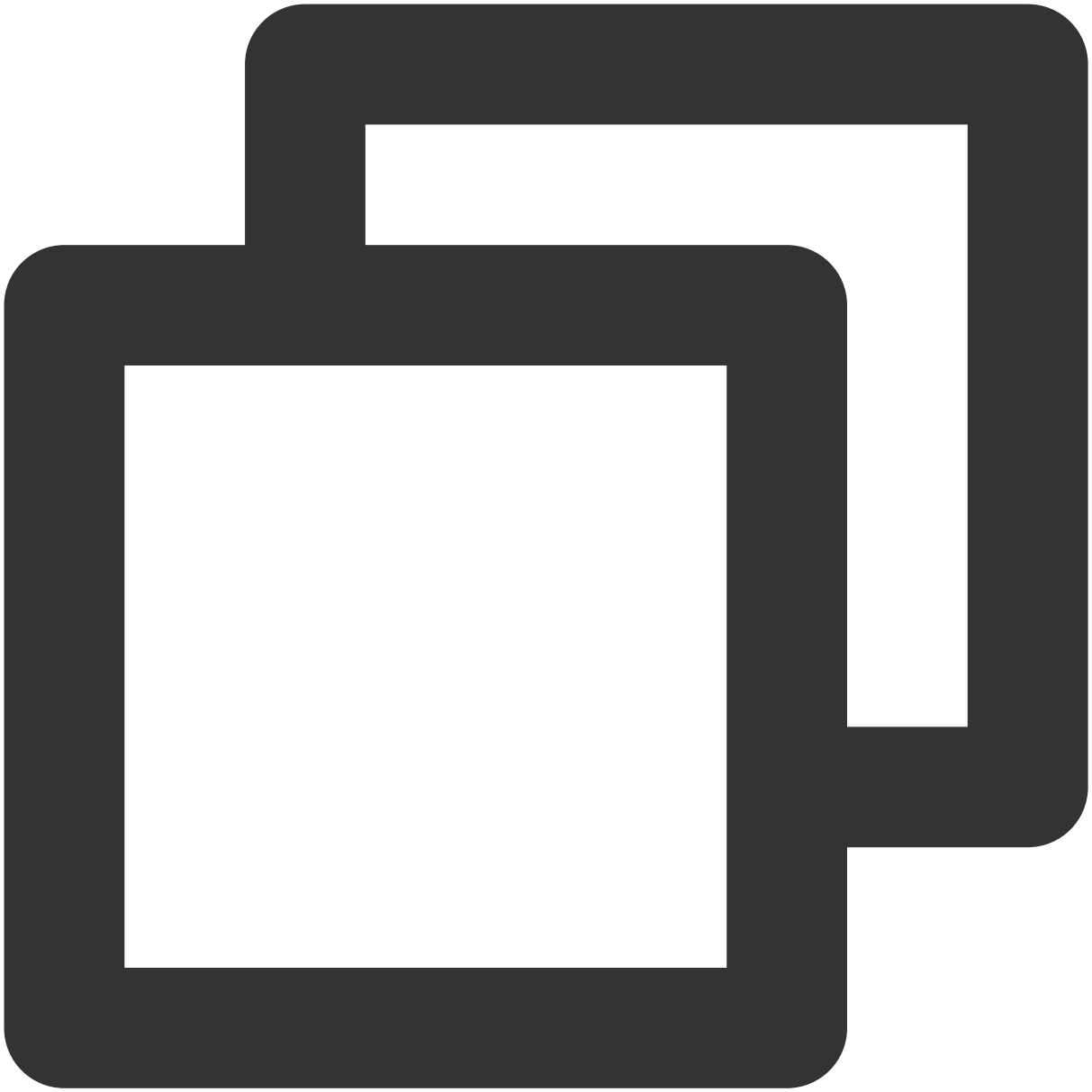
接口描述

注册新用户。此接口适用于**应用系统自行开发注册功能的场景**，如果您的应用使用了 CIAM 认证门户，请参考 使用认证门户注册。
调用此接口前，请确认已配置并启用了应用的注册流程。接口入参需要遵循注册流程中配置的业务规则。例如，注册流程配置了电话号码作为认证属性，用户昵称作为必填普通属性，则入参中必须包含电话号码和用户昵称这两个属性；**如果注册流程未配置电话号码作为认证属性，则入参中不能包含电话号码**。
注册信息中包含电话号码或邮箱地址时，需要先调用 发送 OTP 验证码 接口向用户发送验证码。
密码为可选参数，您可以根据具体业务情况决定是否要求用户设置密码。
如果用户仅通过短信 OTP、邮箱 OTP 或社交认证方式登录，可以不设置密码。
如需支持用户通过账号密码认证登录，则应设置密码。
如果需要设置密码，请确保应用的登录流程中**关联了账号密码认证源**，接口将根据该认证源的密码策略对传入密码进行校验，如果密码不满足策略要求则无法成功完成注册。
说明：
此接口不支持设置用户组。注册成功的用户默认归属注册流程中配置的用户组。
此接口不处理自动登录和实名认证逻辑。即注册流程中的自动登录和实名认证相关配置对此接口不生效。

支持的应用类型

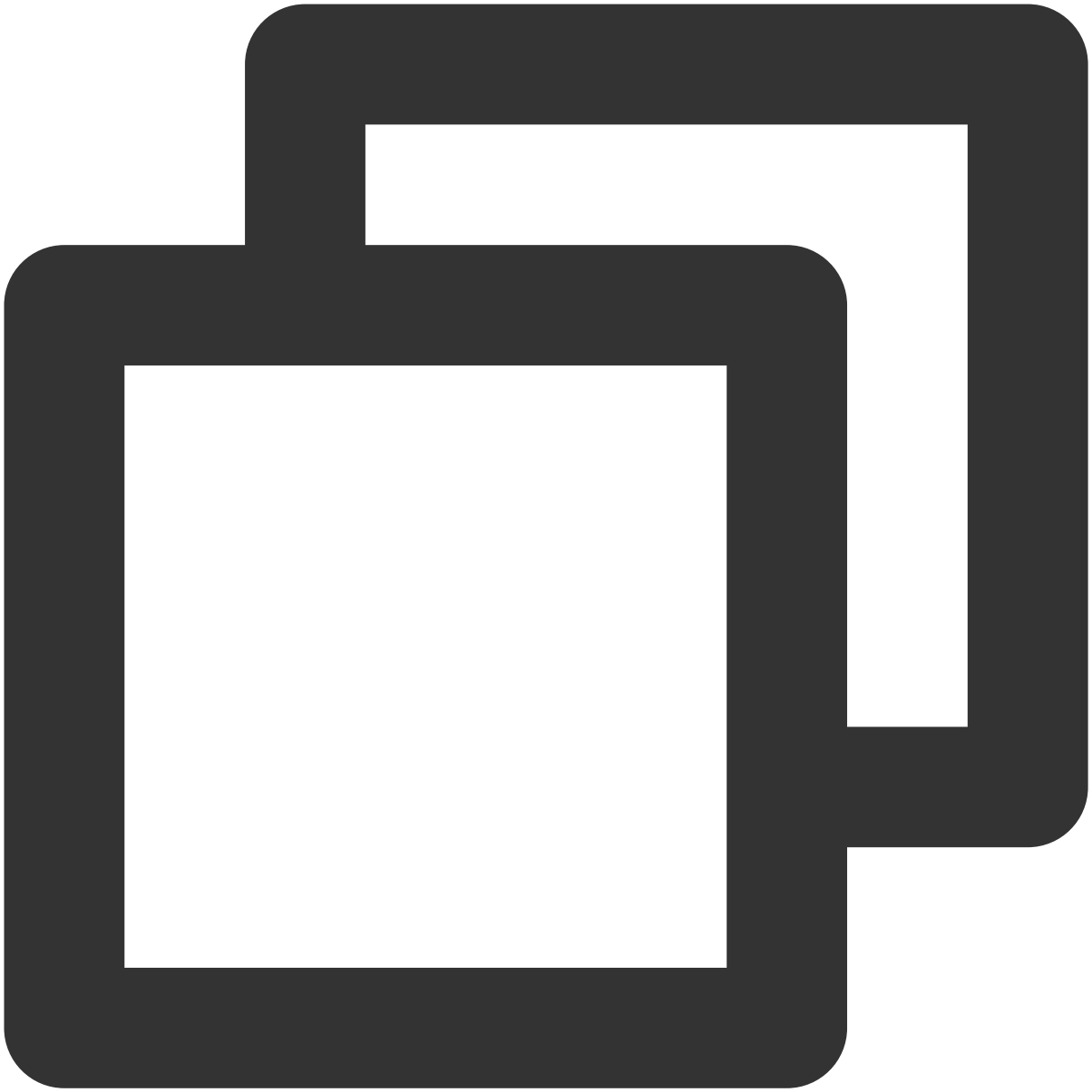
Web 应用。

请求方法



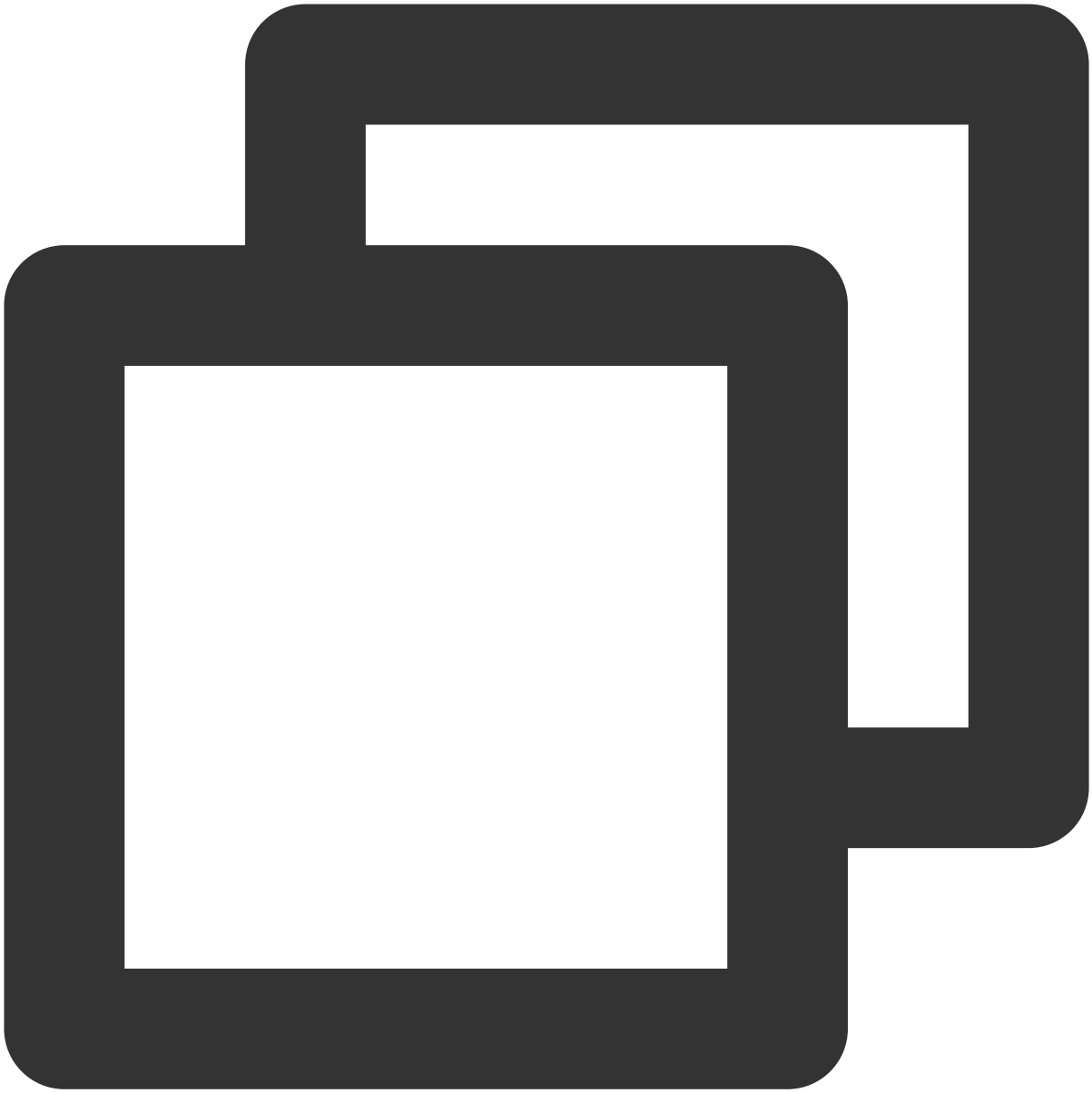
```
POST
```

请求路径



```
/signup
```

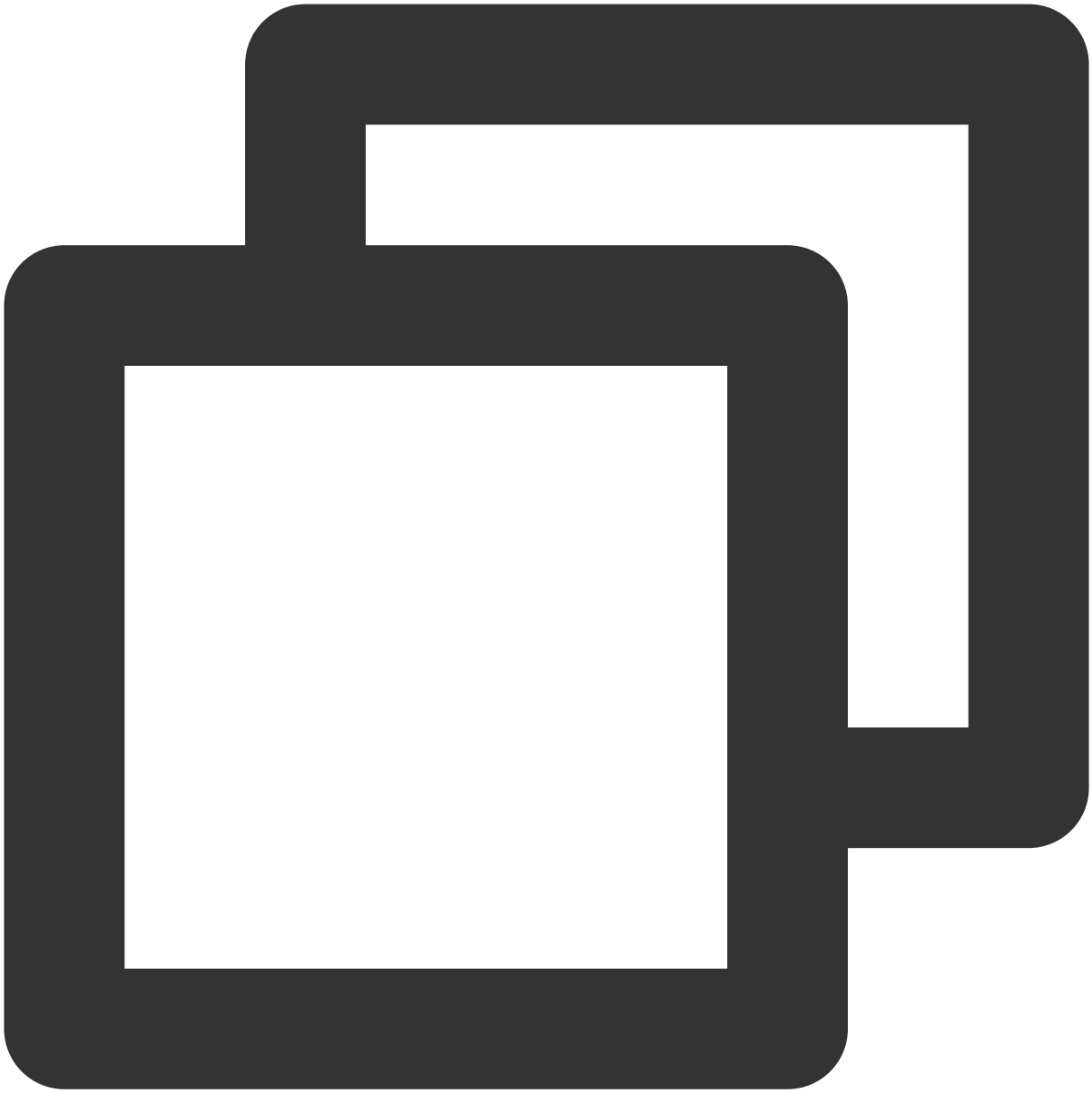
请求 Content-Type



```
application/json
```

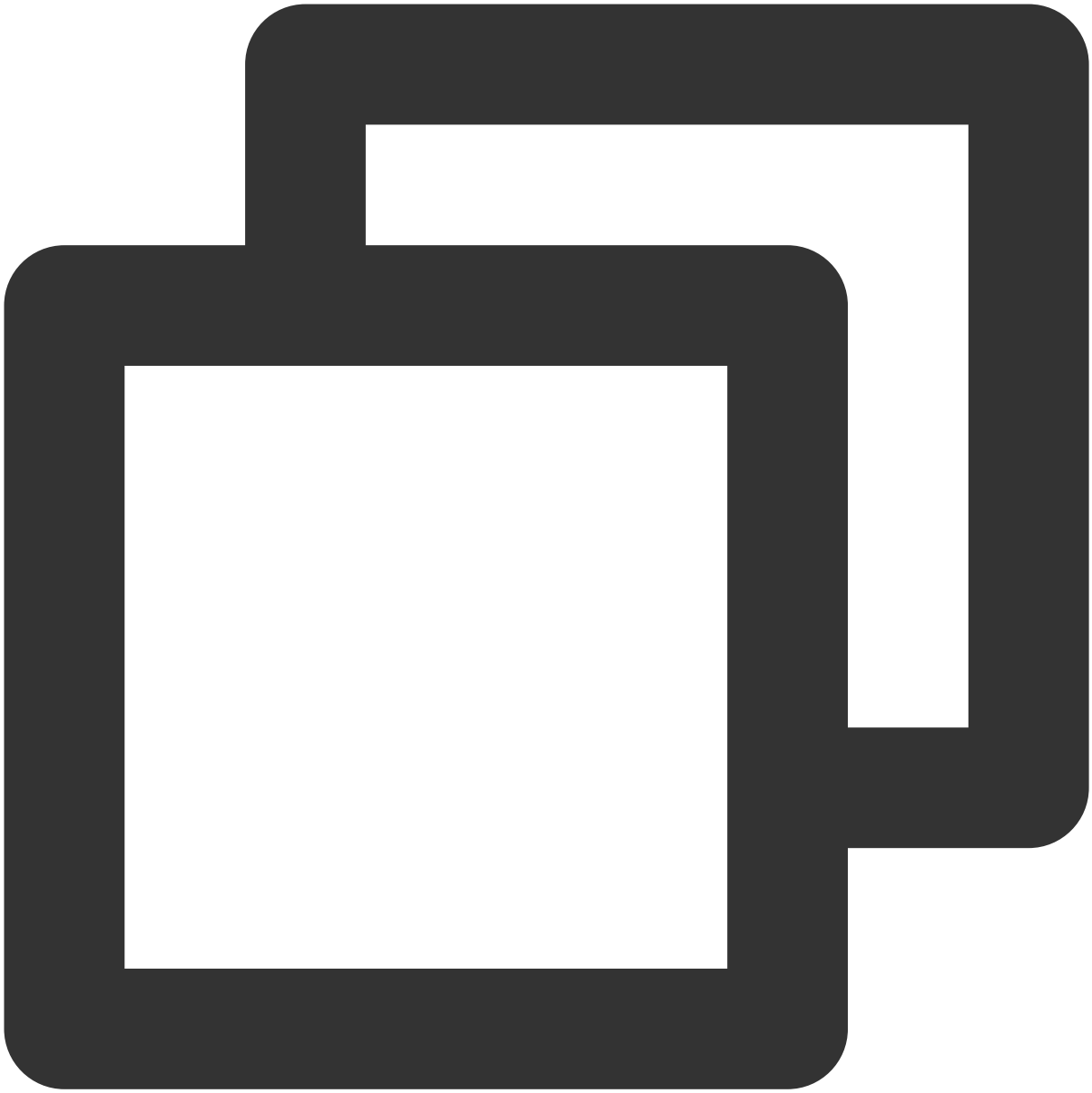
请求示例

使用用户名注册，并设置密码。



```
POST /signup HTTP/1.1
Content-Type: application/json
Authorization: Basic VEVOQU5UX0NMSUVOVF9JRDpURU5BTlRfQ0xJRU5UX1NFQ1JFVA==
Host: sample.portal.tencentciam.com

{
"username" : "MOCK_USERNAME",
"password" : "MOCK_PASSWORD"
}
```

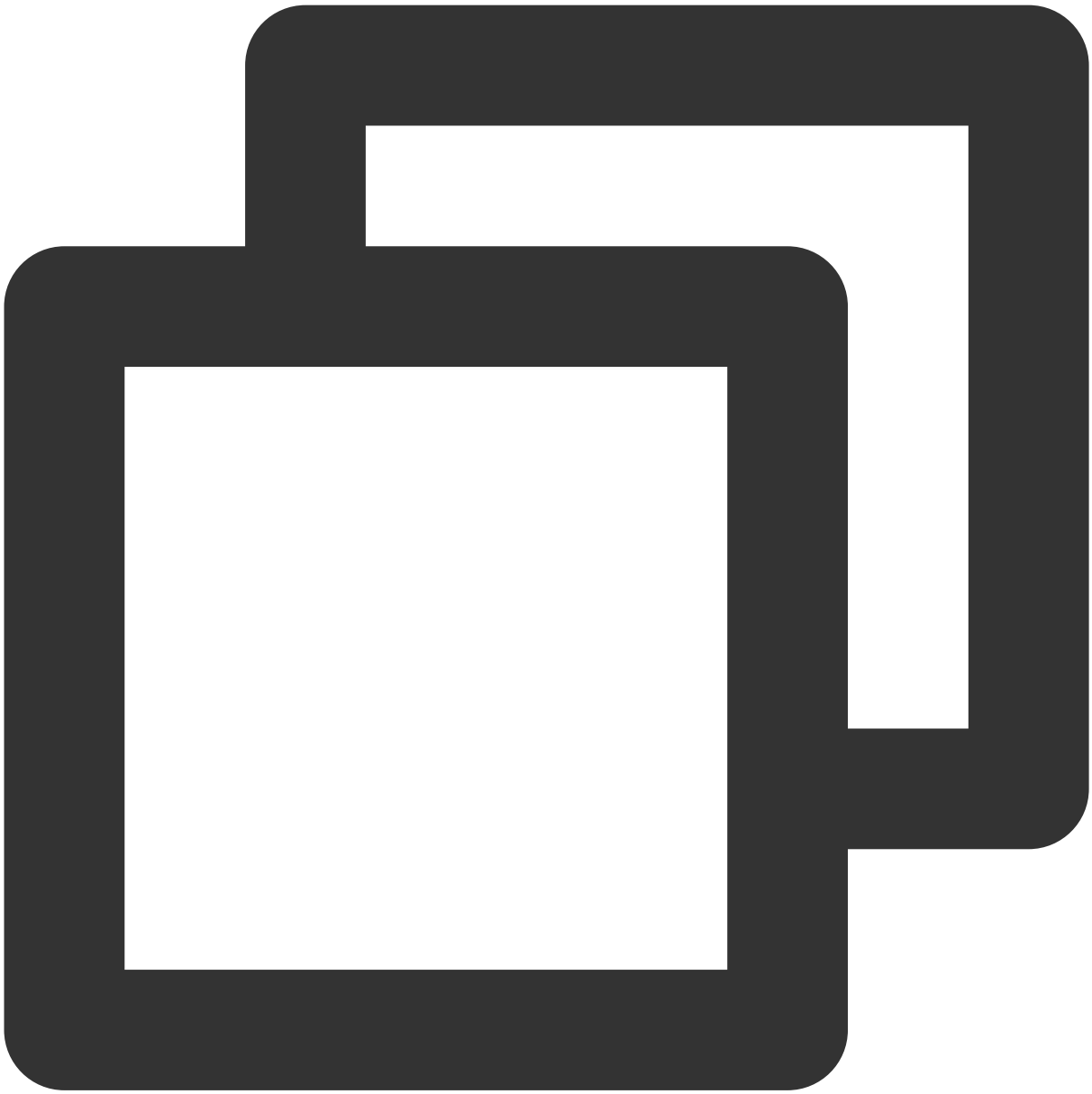
使用邮箱和昵称注册，并设置密码。



```
POST /signup HTTP/1.1
Content-Type: application/json
Authorization: Basic VEVOQU5UX0NMSUVOVF9JRDpURU5BTlRfQ0xJRU5UX1NFQ1JFVA==
Host: sample.portal.tencentciam.com

{
"email" : "MOCK_USERNAME@example.com",
"email_otp_token" : "MOCK_EMAIL_OTP_TOKEN",
"email_otp" : "MOCK_EMAIL_OTP",
"password" : "MOCK_PASSWORD",
"nickname" : "MOCK_NICKNAME"
```

```
}
```

使用电话号码注册，不设置密码。



```
POST /signup HTTP/1.1
Content-Type: application/json
Authorization: Basic VEVOQU5UX0NMSUVOVF9JRDpURU5BTlRfQ0xJRU5UX1NFQ1JFVA==
Host: sample.portal.tencentciam.com

{
"phone_number" : "13612345678",
"phone_number_otp_token" : "MOCK_PHONE_NUMBER_OTP_TOKEN",
```

```
"phone_number_otp" : "MOCK_PHONE_NUMBER_OTP"
}
```

请求头

名称	描述
Authorization	HTTP Basic 认证请求头，格式为 `Basic <credentials>` ，其中 `Basic` 为固定字符串， `<credentials>` 的计算方式为 `base64(url_encode(client_id) + ":" + url_encode(client_secret))` ， `Basic` 和 `<credentials>` 之间用一个空格隔开。

请求体 JSON 参数

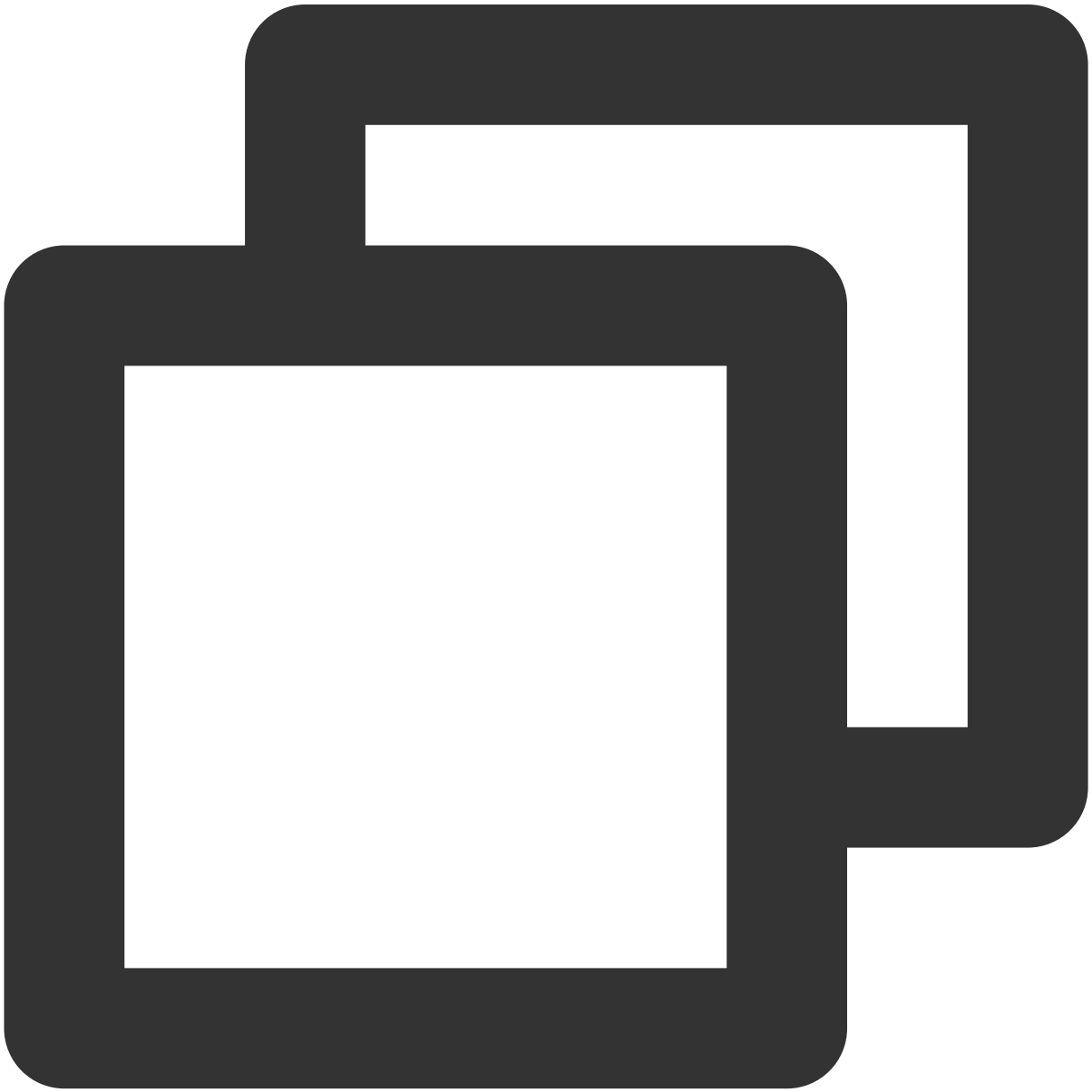
JSON 路径	数据类型	描述
username	String	用户名，可以包含英文字母、数字和下划线，必须以字母开始，最长32个字符。
password	String	用户密码。如果设置，则必须符合应用关联的账号密码认证源的密码策略。
phone_number	String	用户的手机号，限国内三大运营商11位手机号。传递此参数时，须同时传递 `phone_number_otp_token` 和 `phone_number_otp` 两个参数。
phone_number_otp_token	String	发送短信验证码成功后服务端返回的 `otp_token` 。
phone_number_otp	String	用户手机收到的 OTP 验证码。
email	String	用户的邮箱地址。传递此参数时，须同时传递 `email_otp_token` 和 `email_otp` 两个参数。
email_otp_token	String	发送邮箱验证码成功后服务端返回的 `otp_token` 。
email_otp	String	用户邮箱收到的 OTP 验证码。
name	String	用户姓名。
nickname	String	用户昵称。

zoneinfo	String	用户时区，如 `Asia/Shanghai` 或 `Europe/Paris` 。
locale	String	用户 locale 信息，如 `zh-CN` 或 `en-US` 。

说明：

其他参数的取值为用户属性标识。属性标识可以在 属性自定义页面 的属性详情界面查看。

注册成功响应示例



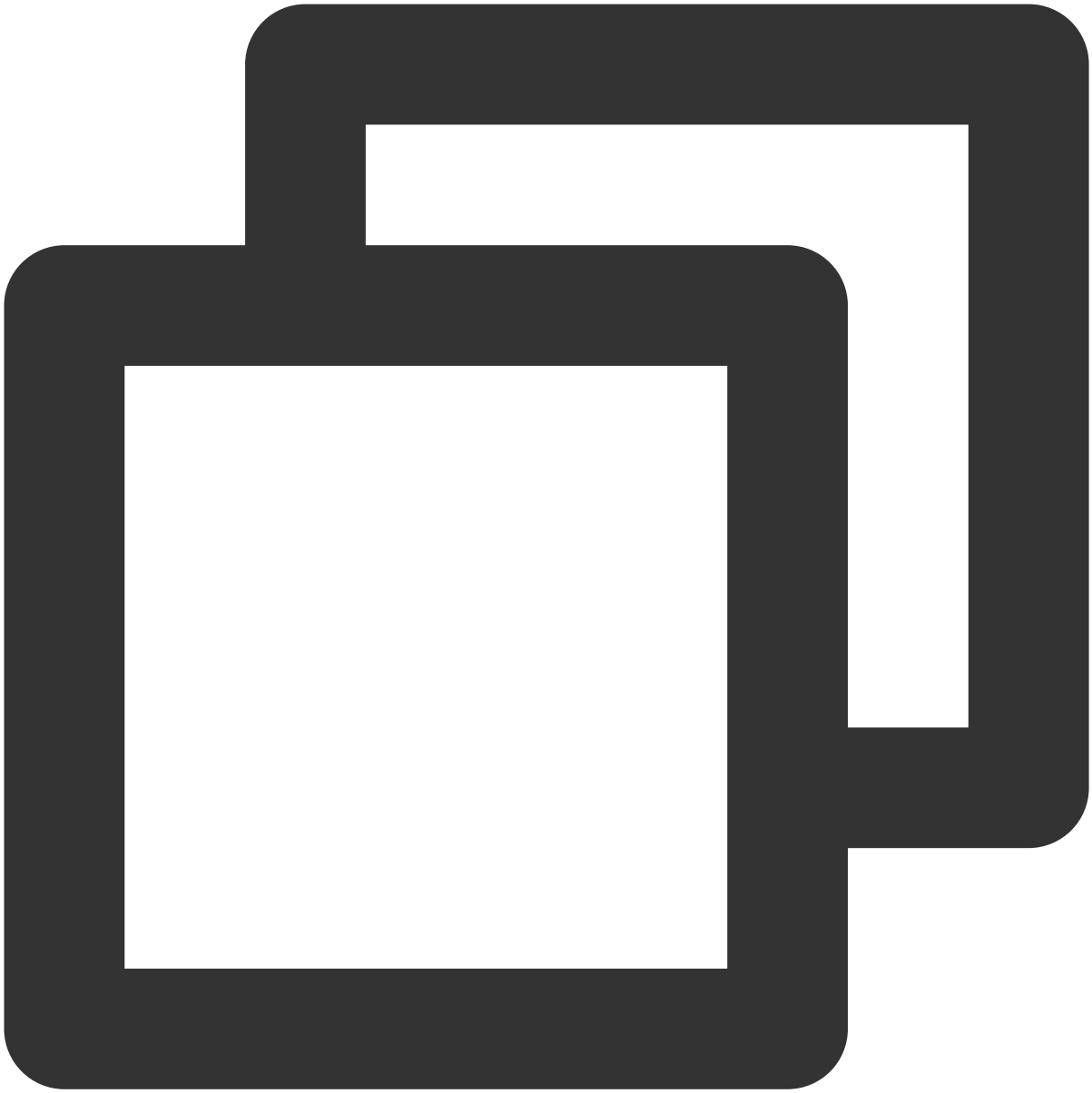
```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "sub" : "MOCK_USER_ID"
}
```

响应参数

字段	数据类型	描述
sub	String	用户唯一标识。

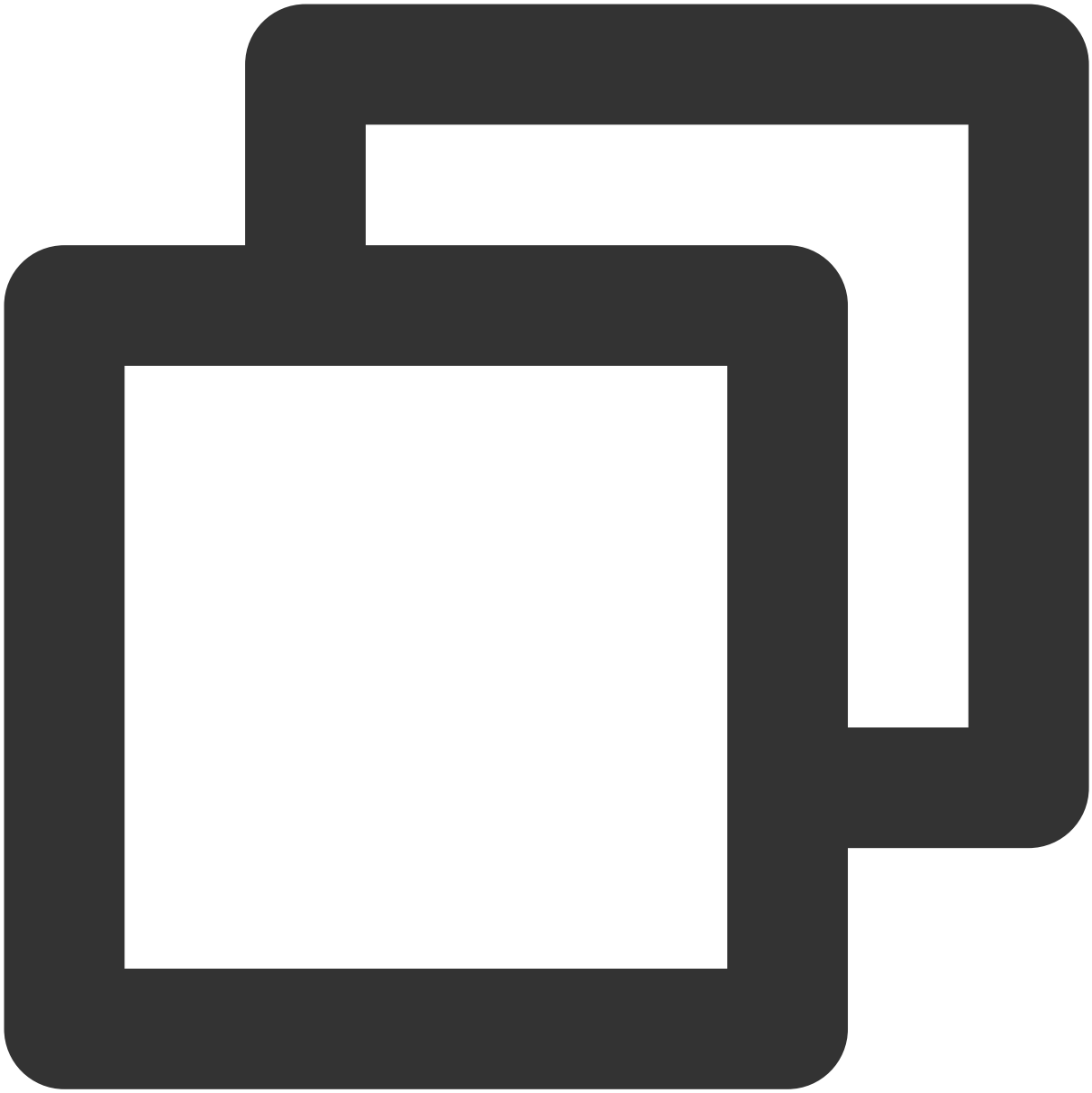
注册失败响应示例

应用注册流程未启用。



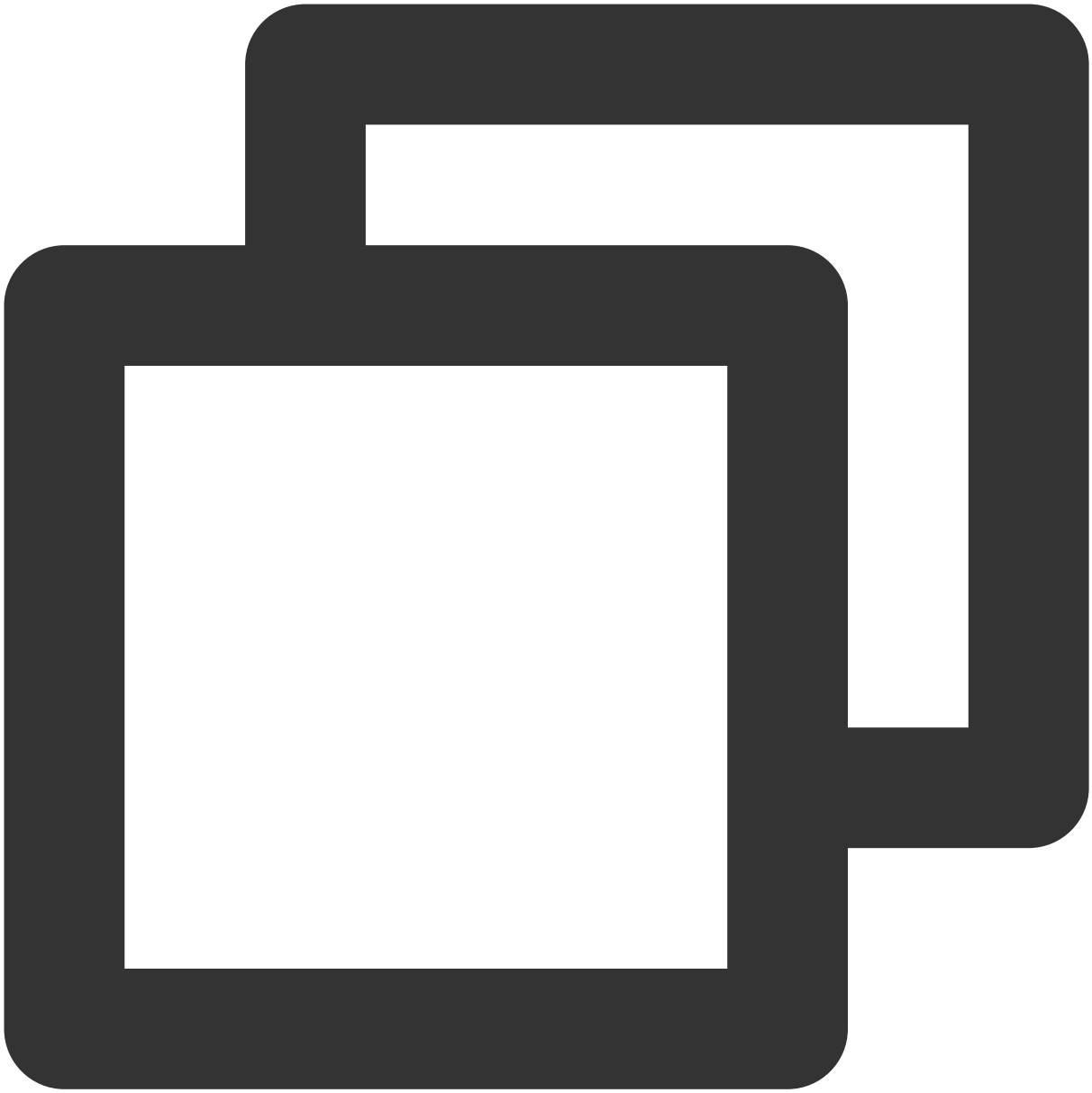
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "misconfigured",
"error_description" : "Sign up flow of the application is not enabled."
}
```

入参缺少注册流程配置的认证属性或必填普通属性。



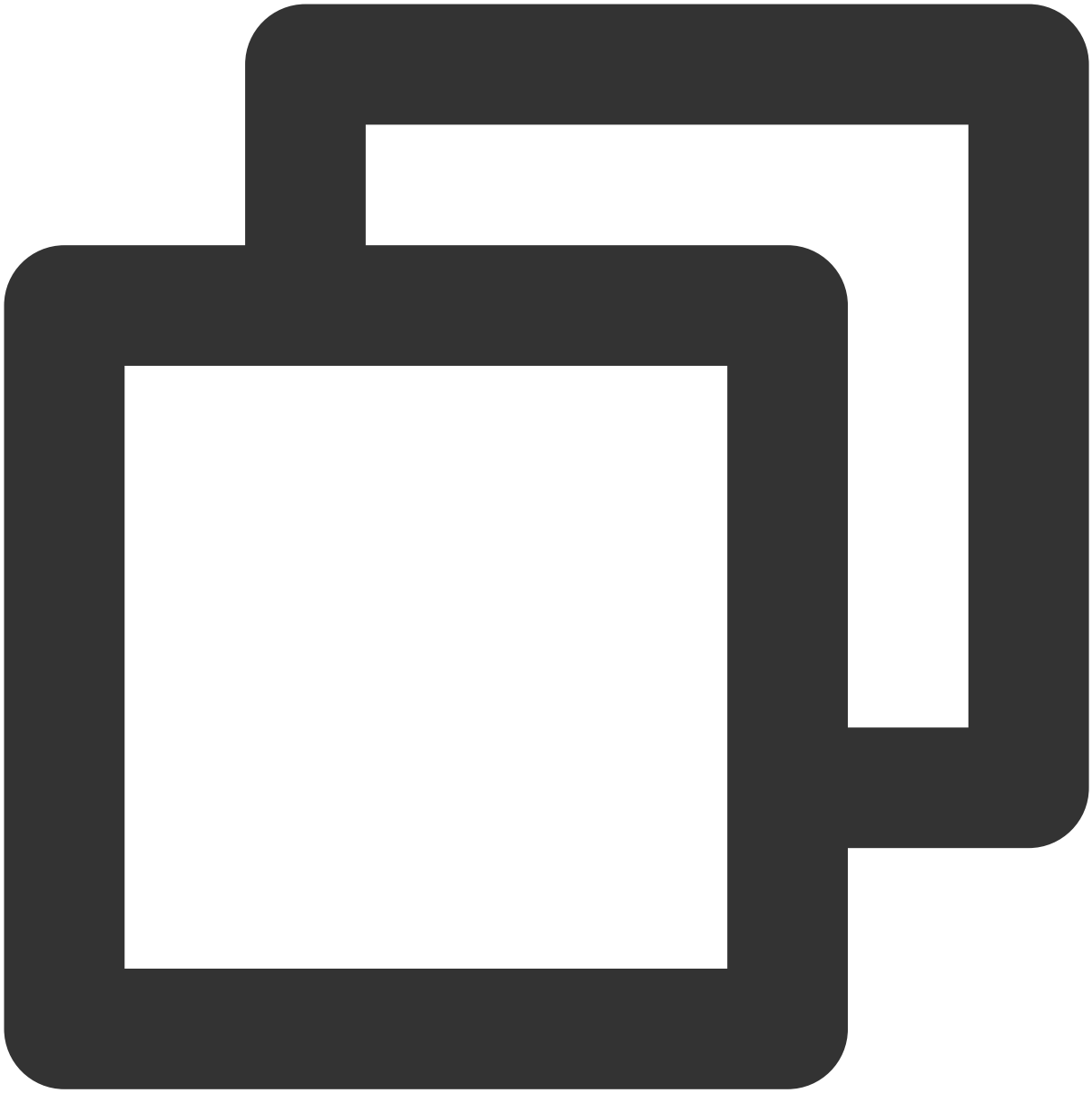
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_request",
"error_description" : "Missing required sign-up attribute(s)."
}
```

入参包含注册流程未配置的认证属性或普通属性。



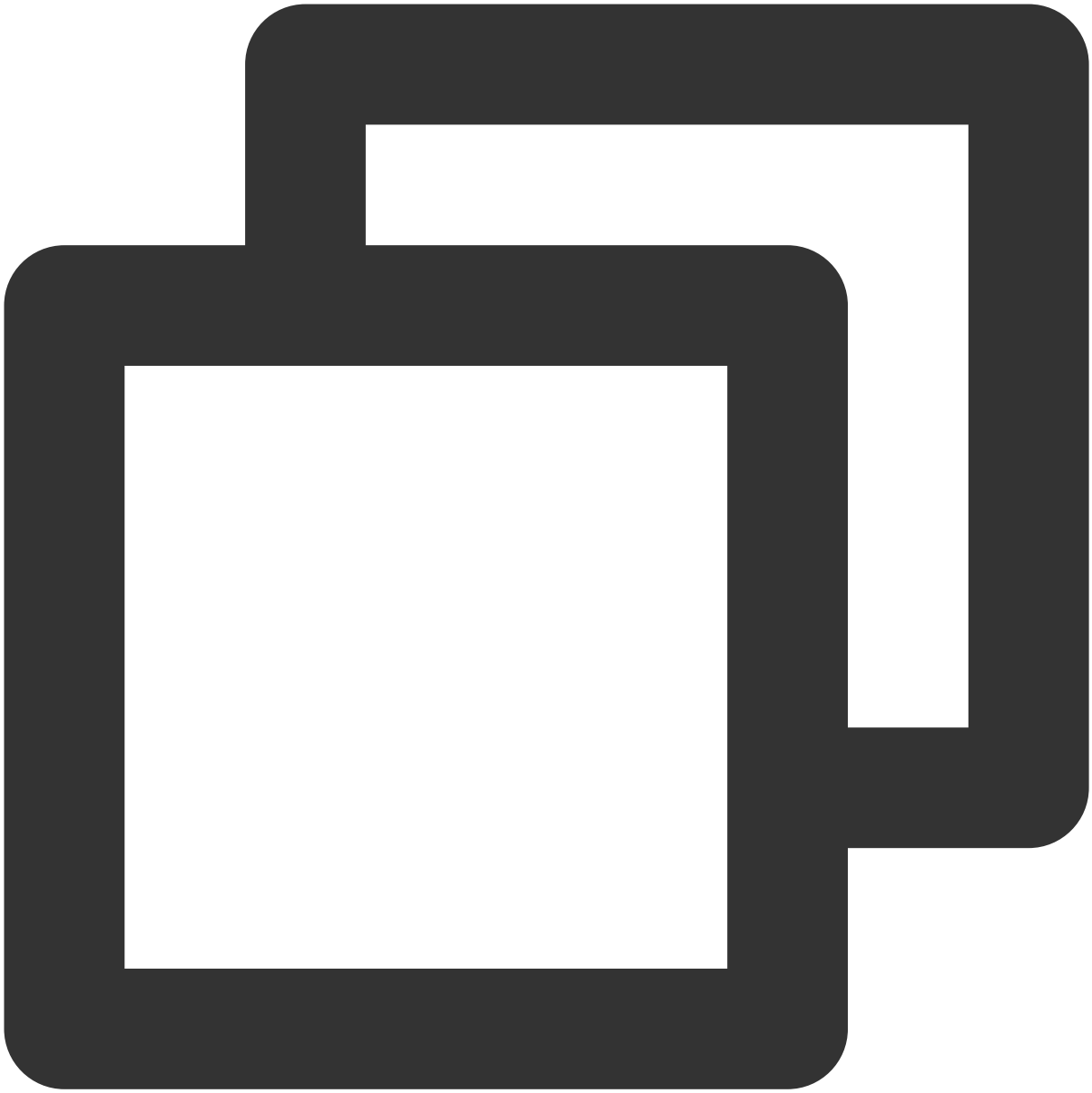
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_request",
"error_description" : "Unconfigured sign-up attribute(s) found."
}
```

入参包含未知属性。



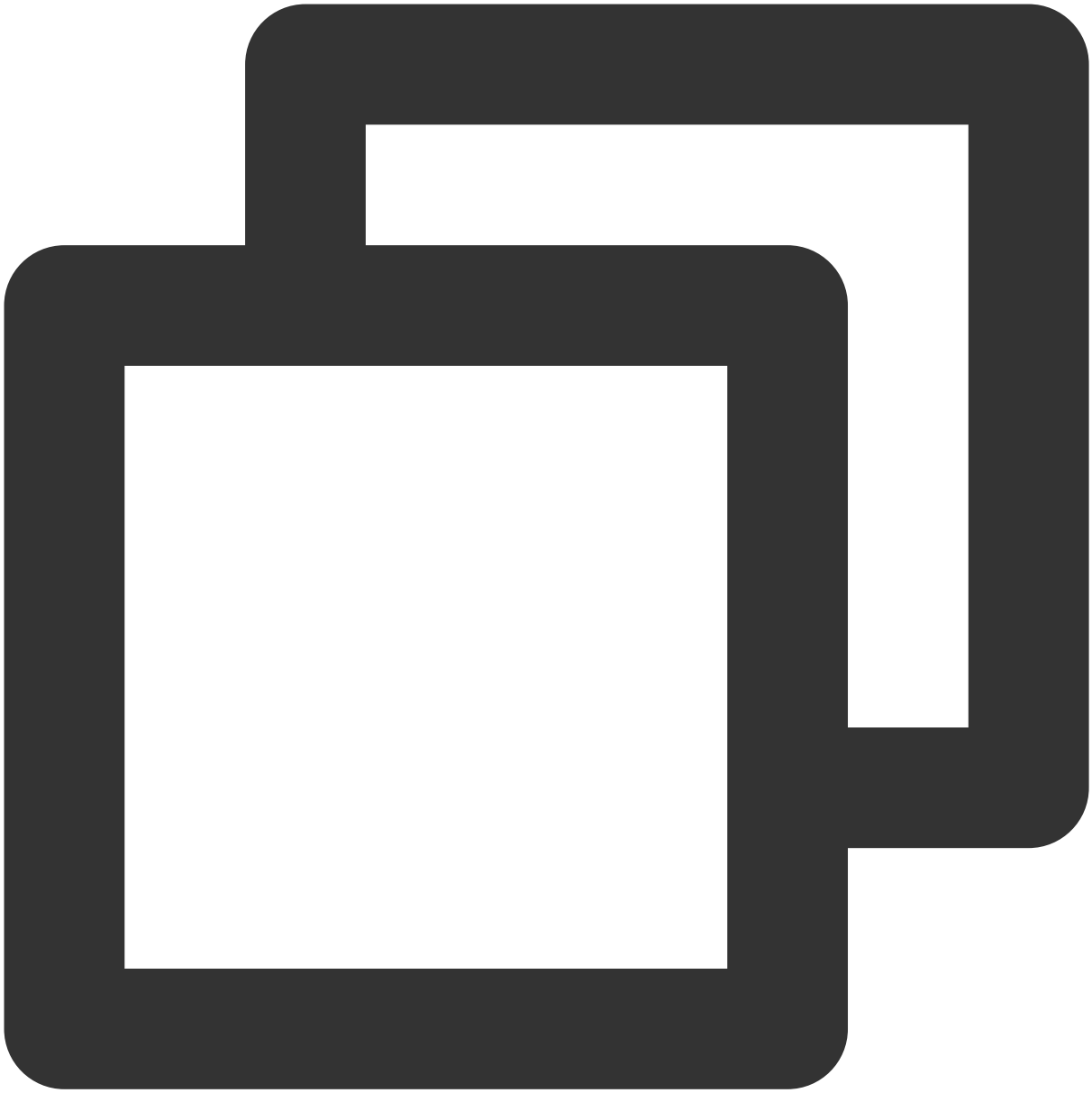
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_request",
"error_description" : "Unknown attribute(s) found."
}
```

用户名格式不合法。



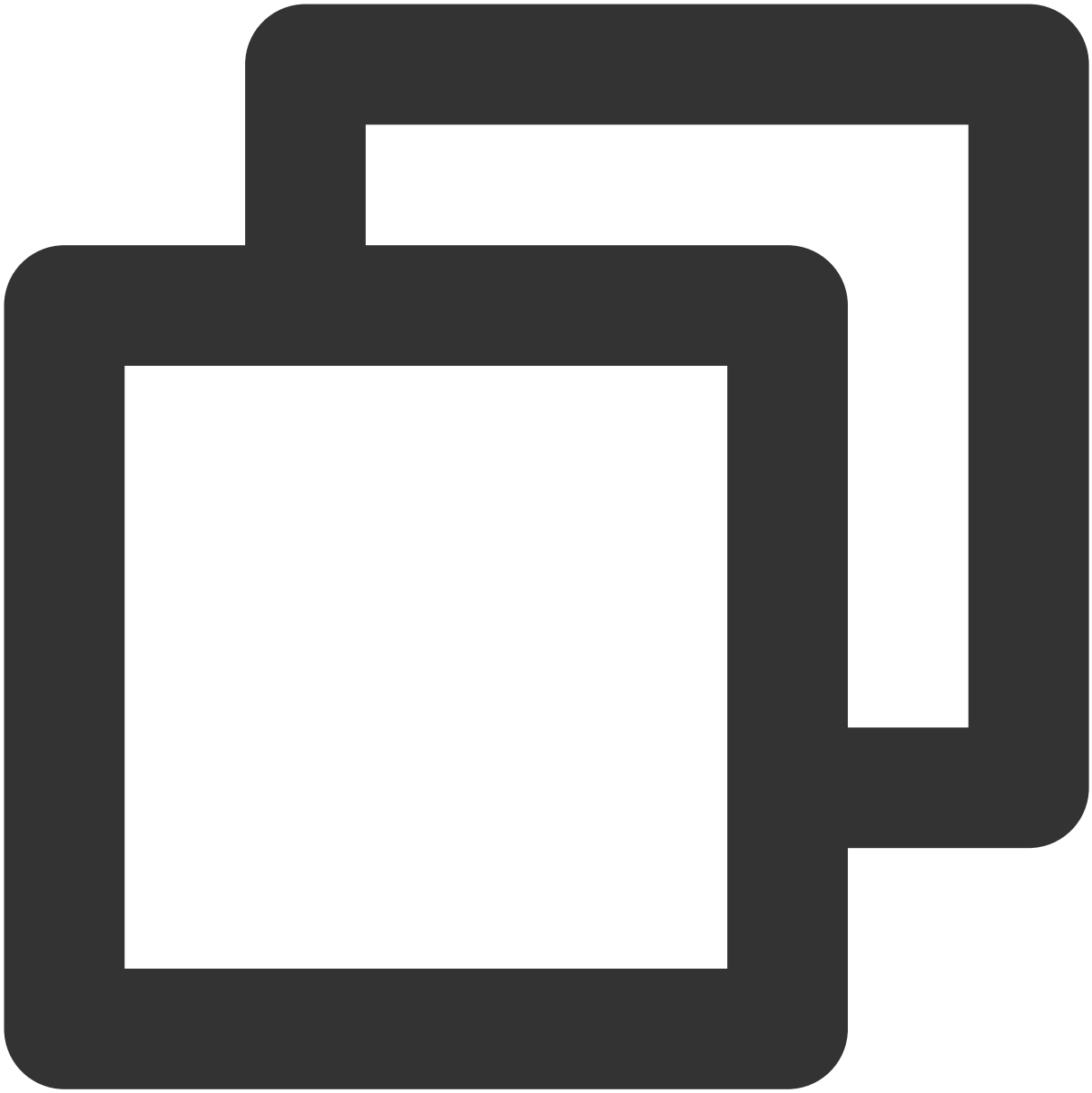
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_username"
}
```

用户名已存在。



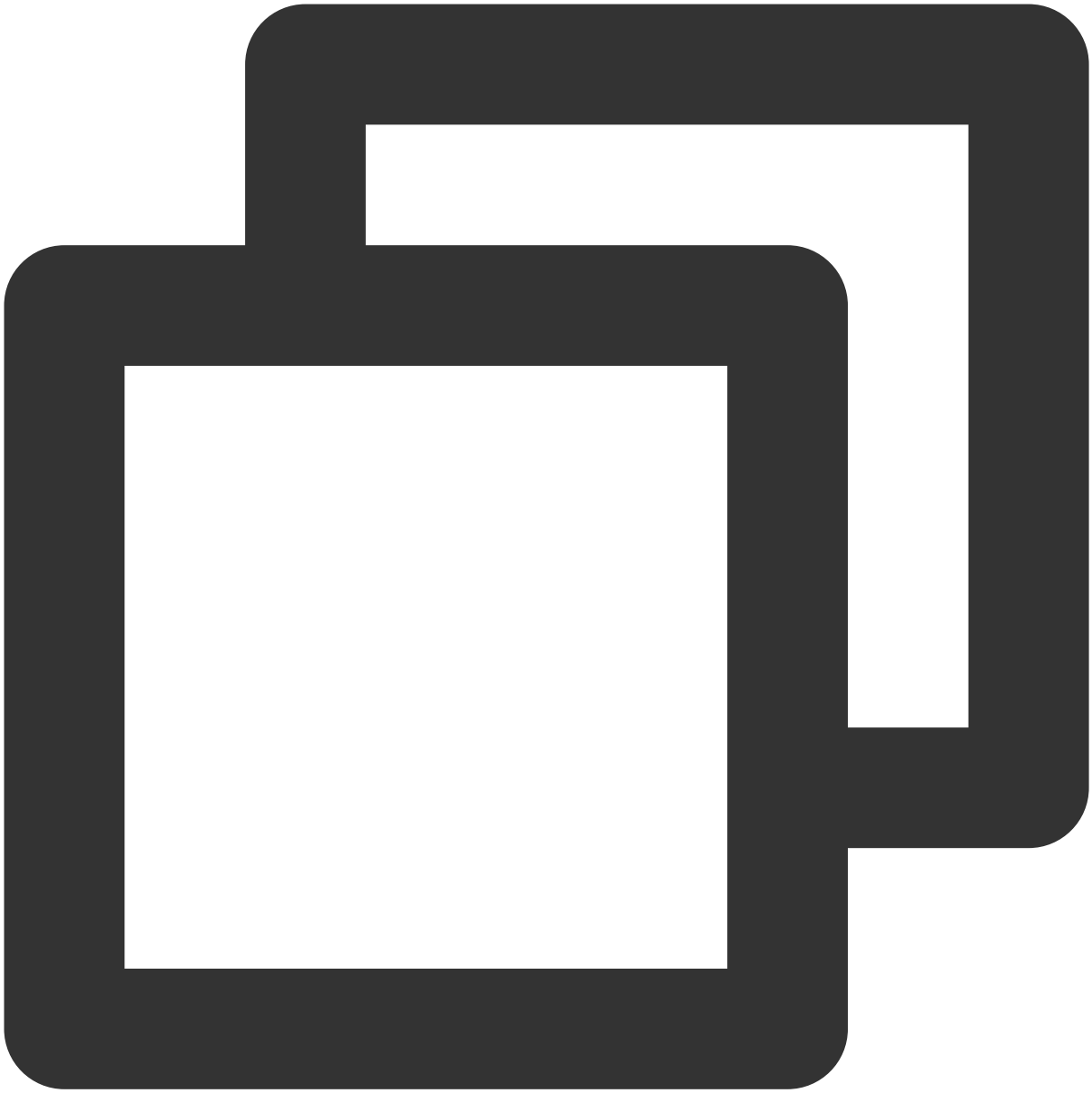
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_username"
}
```

电话号码格式不合法。



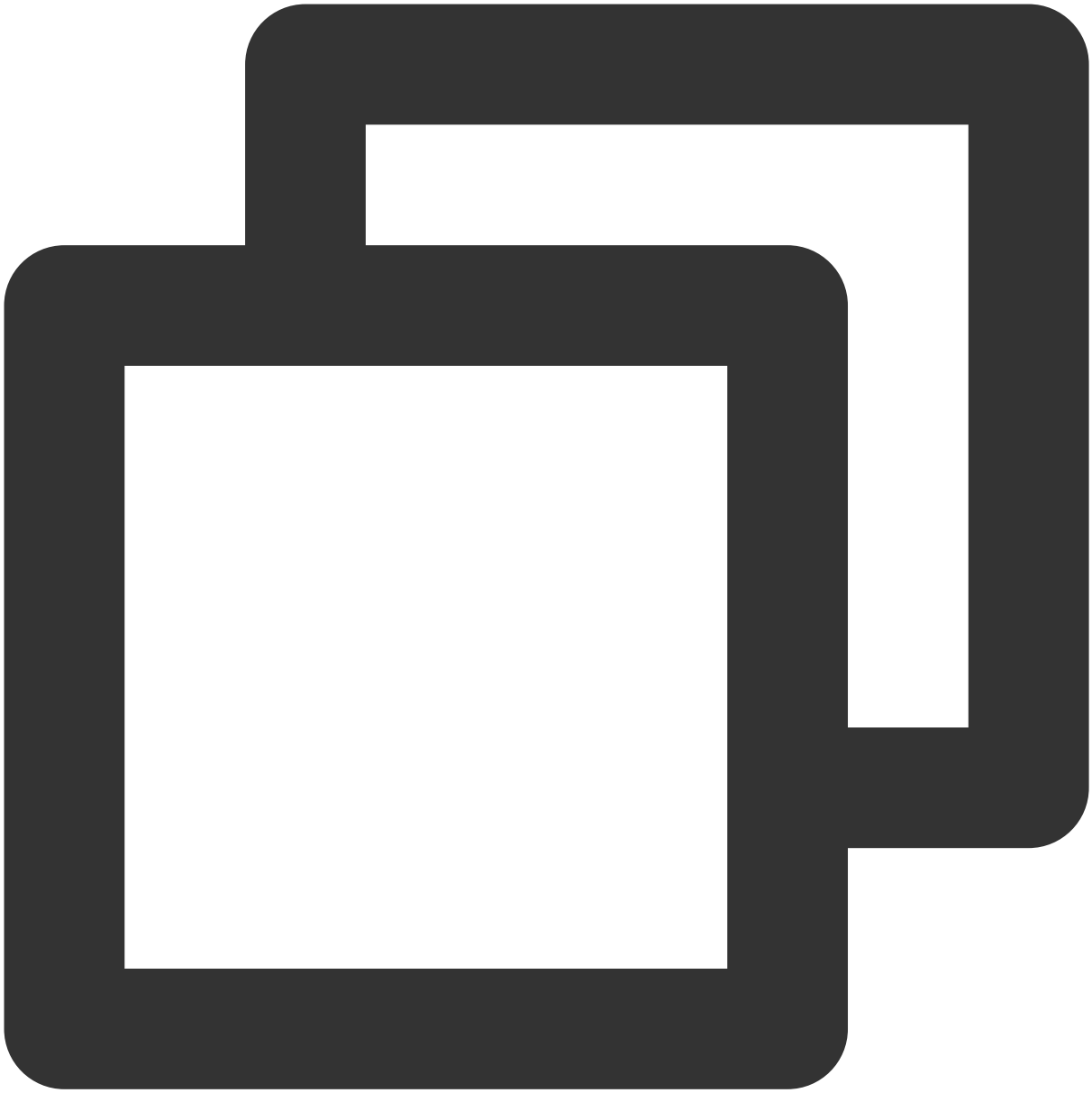
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "malformed_phone_number"
}
```

电话号码已存在。



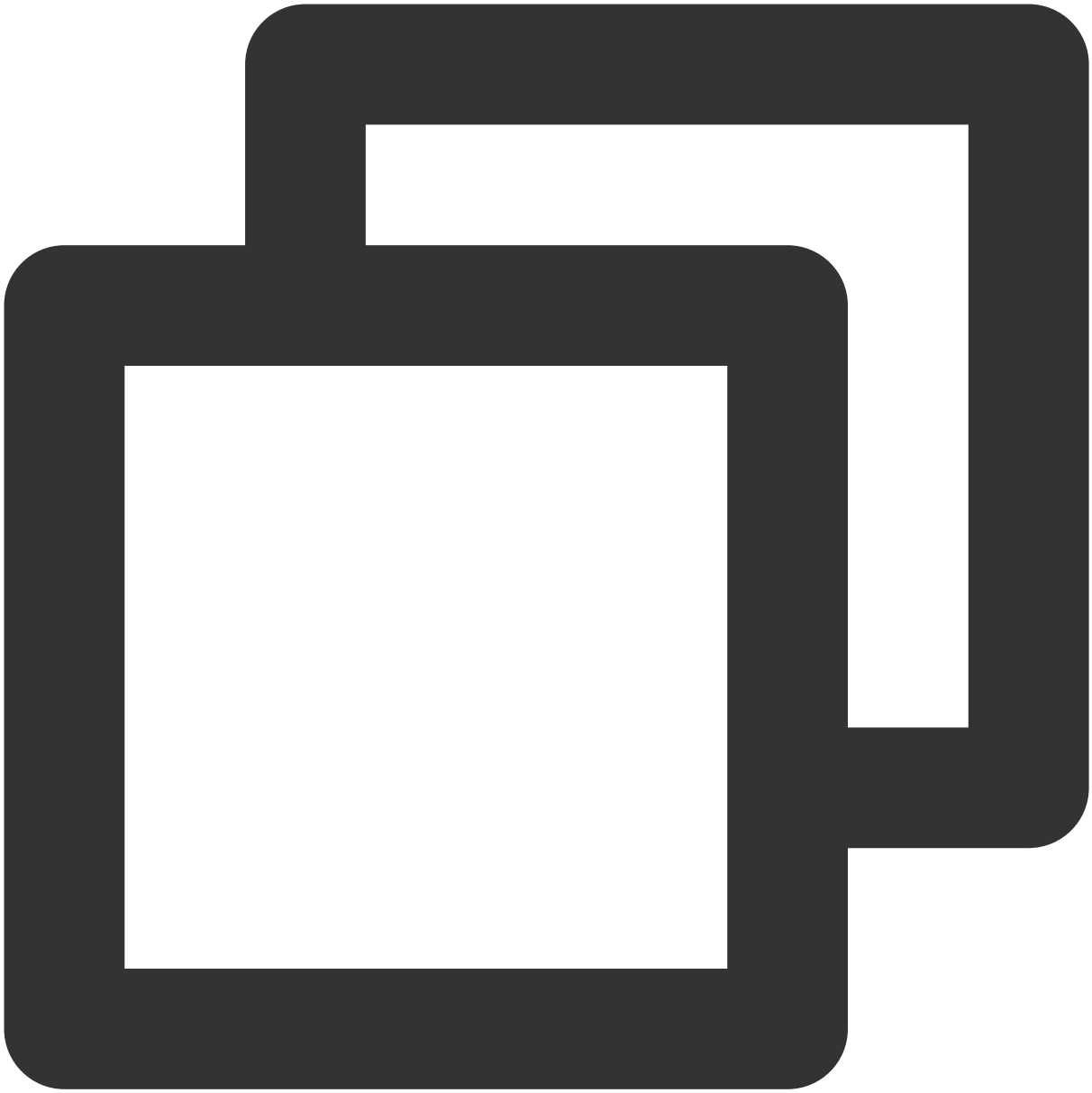
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_phone_number"
}
```

`phone_number_otp_token` 错误或已过期，或注册时使用的参数与发送验证码时不一致（例如：手机号不同）。



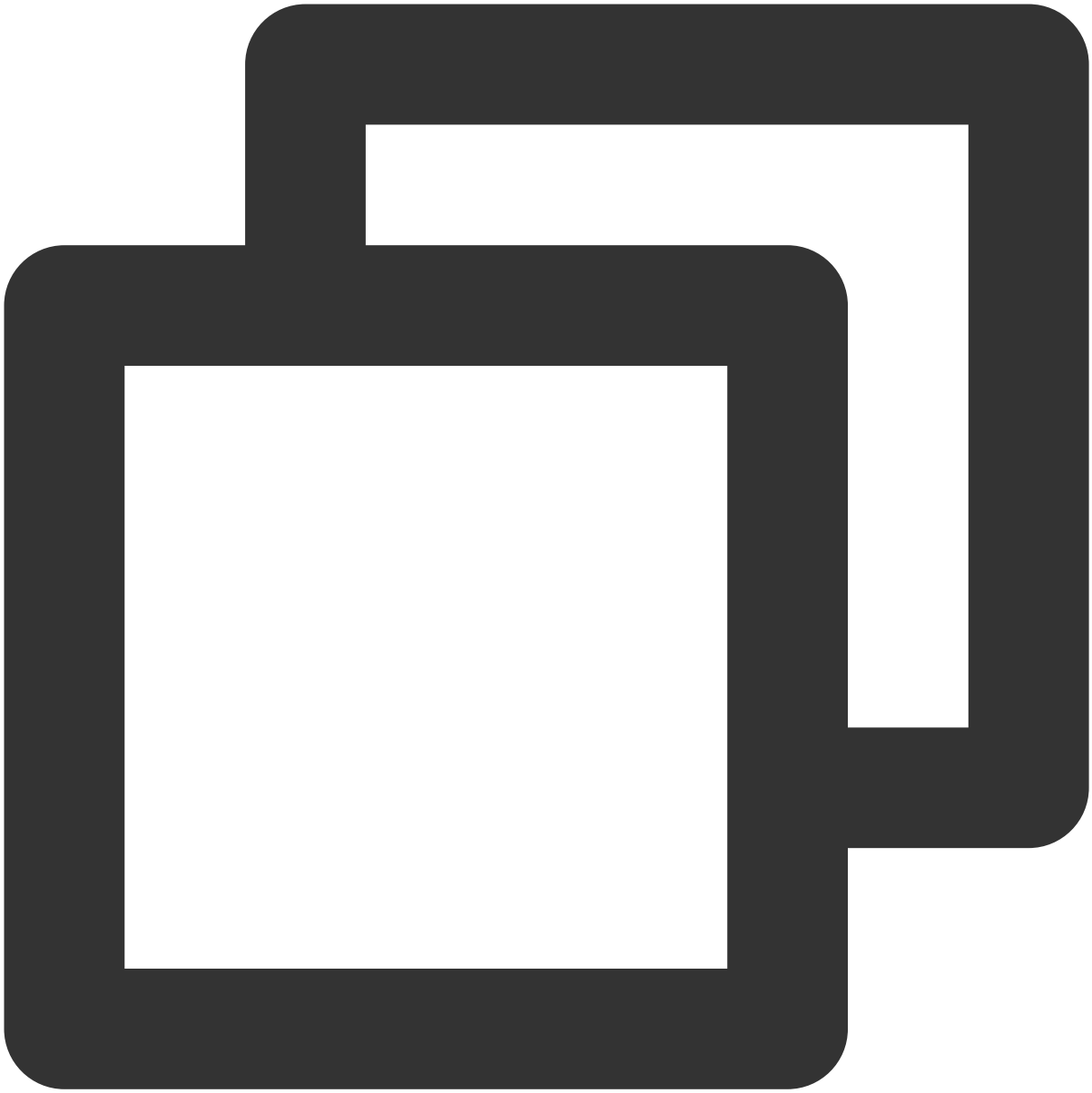
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_phone_number_otp_token"
}
```

`phone_number_otp` 错误或已过期。



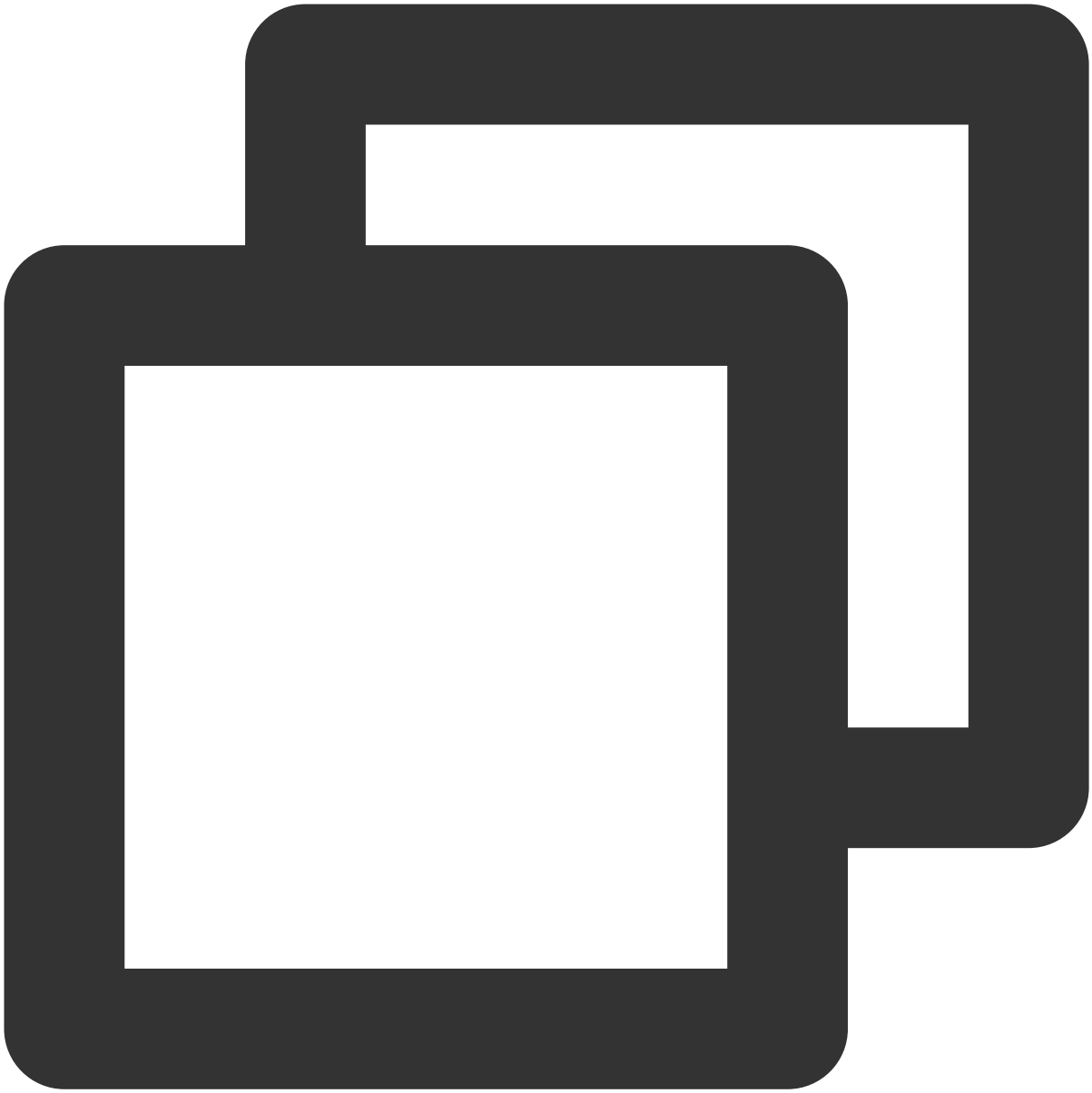
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_phone_number_otp"
}
```

邮箱格式不合法。



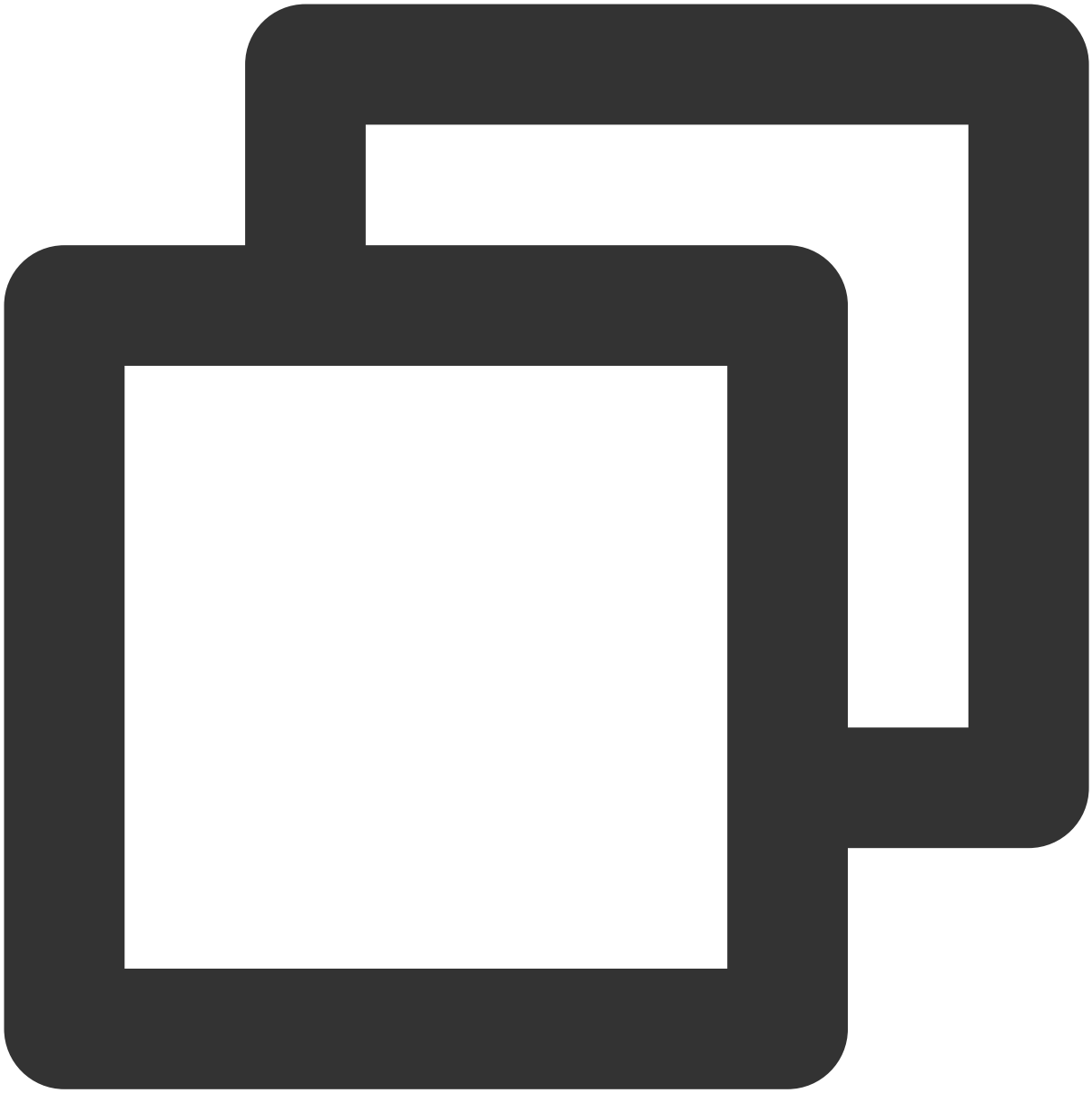
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "malformed_email"
}
```

邮箱已存在。



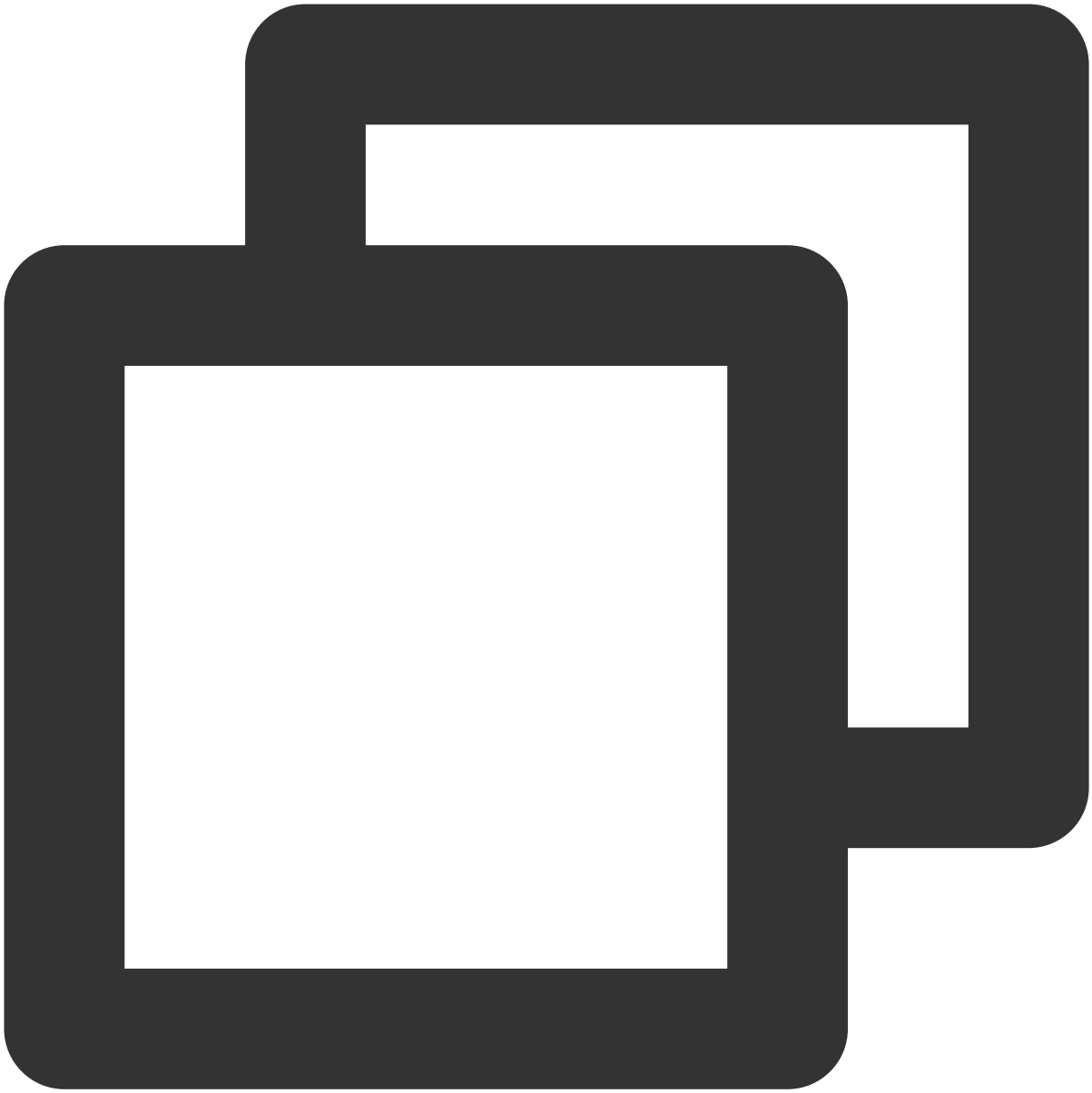
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_email"
}
```

`email_otp_token` 错误或已过期，或注册时使用的参数与发送验证码时不一致（例如：邮箱不同）。



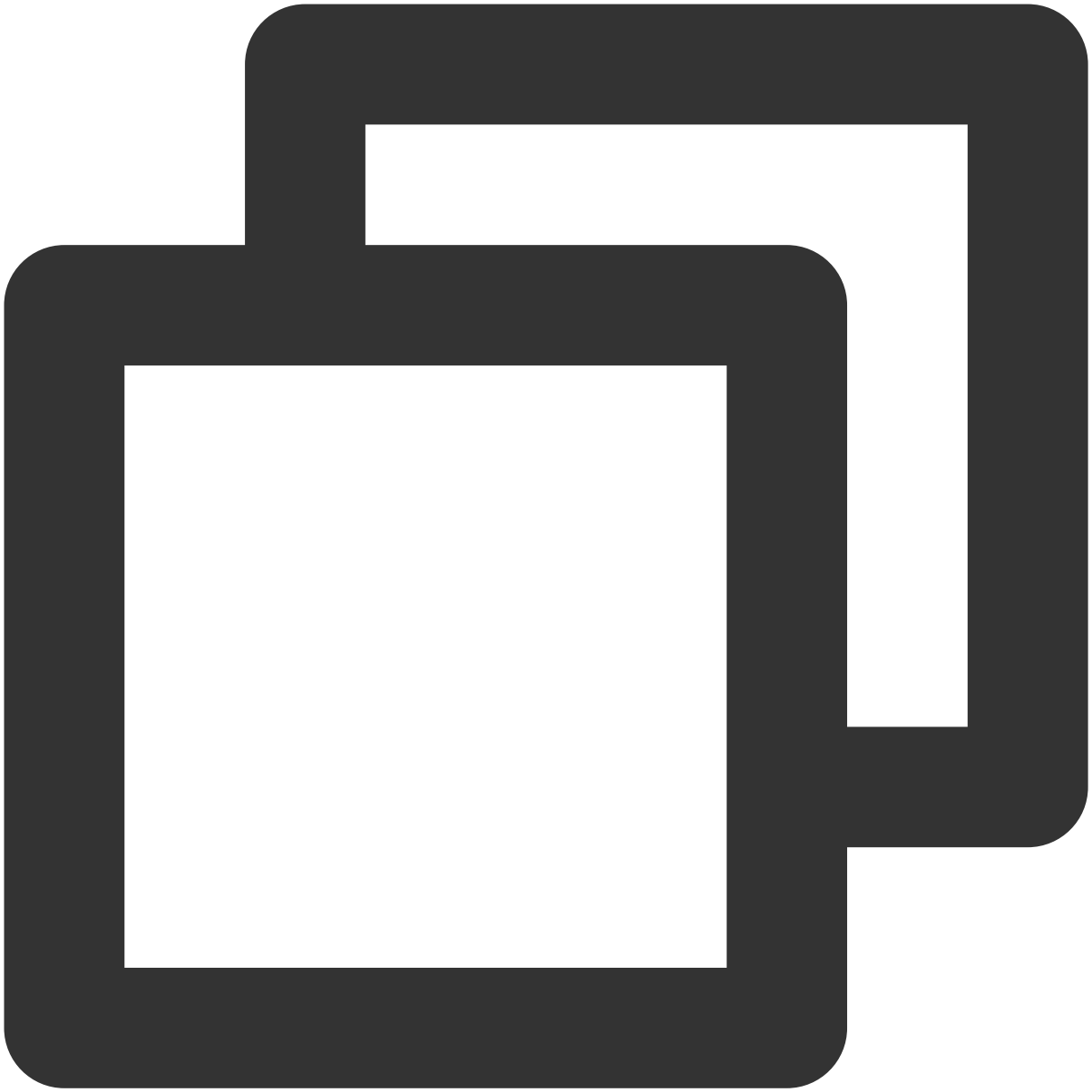
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp_token"
}
```

`email_otp` 错误或已过期。



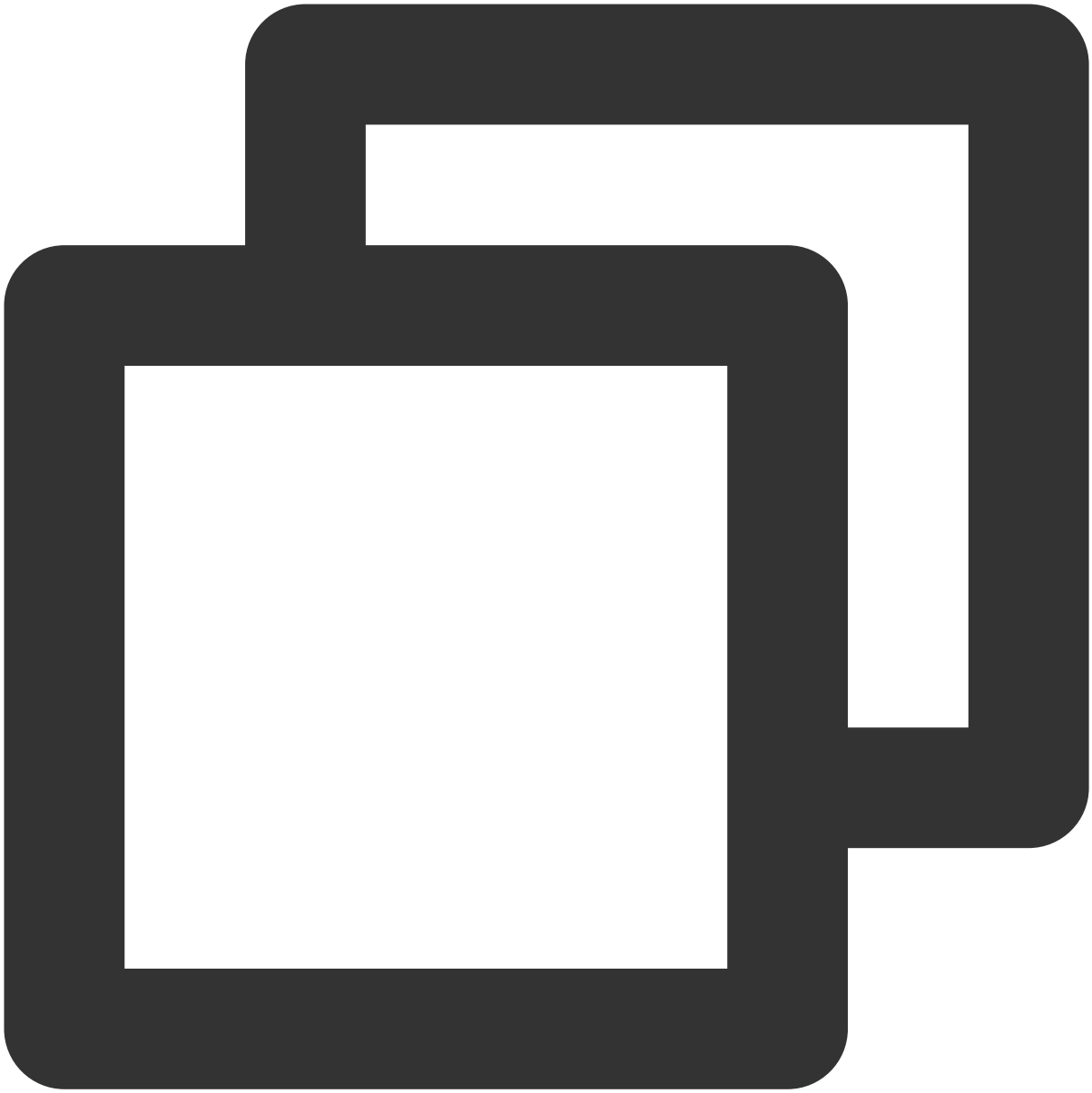
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp"
}
```

入参中传入了密码，但应用登录流程中未关联账号密码认证源。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "misconfigured",
"error_description" : "No password auth source is associated with the application."
}
```

密码不满足策略要求。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_password"
}
```

账号密码认证

最近更新时间：2023-12-22 11:42:08

接口描述

校验用户的用户名和密码，获取 Access Token 和 ID Token，完成登录。此接口对应 OAuth 2.0 协议的 Resource Owner Password Credentials 模式。

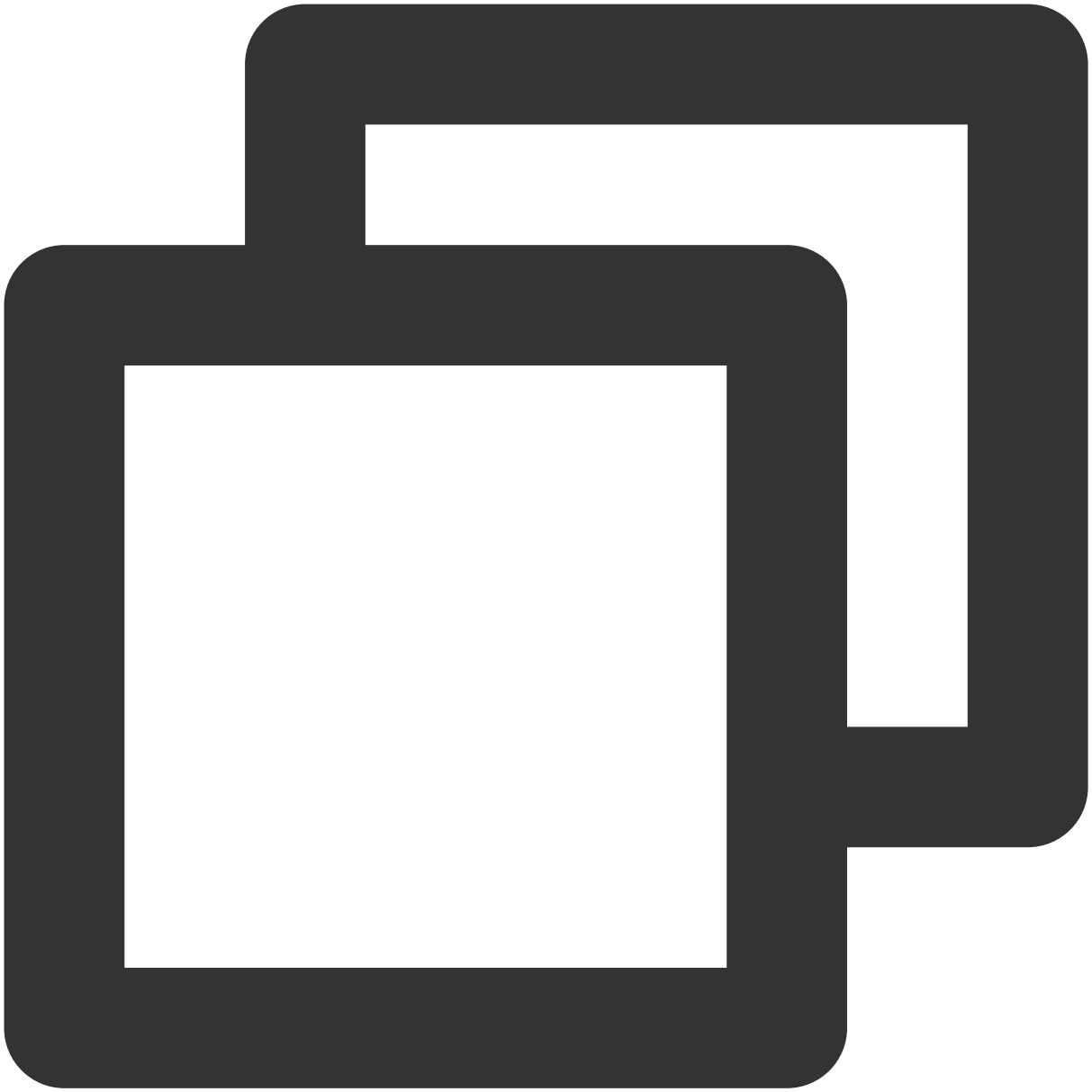
说明：

由于用户密码将在用户终端与应用之间传递，请务必使用高度可信的应用调用此接口，并妥善处理密码的传输（例如确保使用了 HTTPS 协议）。在条件允许的情况下，建议优先使用 认证门户登录。

支持的应用类型

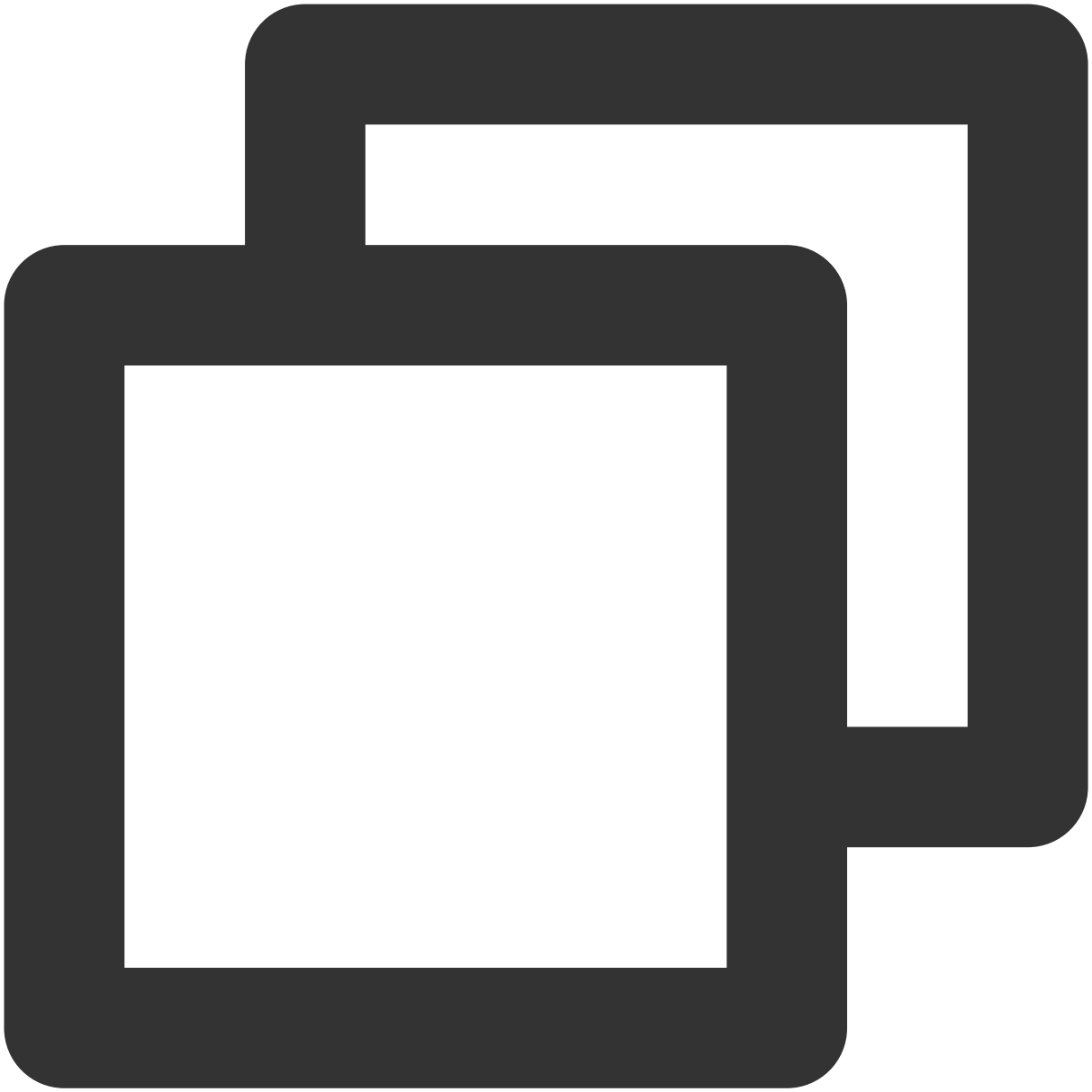
Web 应用、单页应用、移动 App。

请求方法



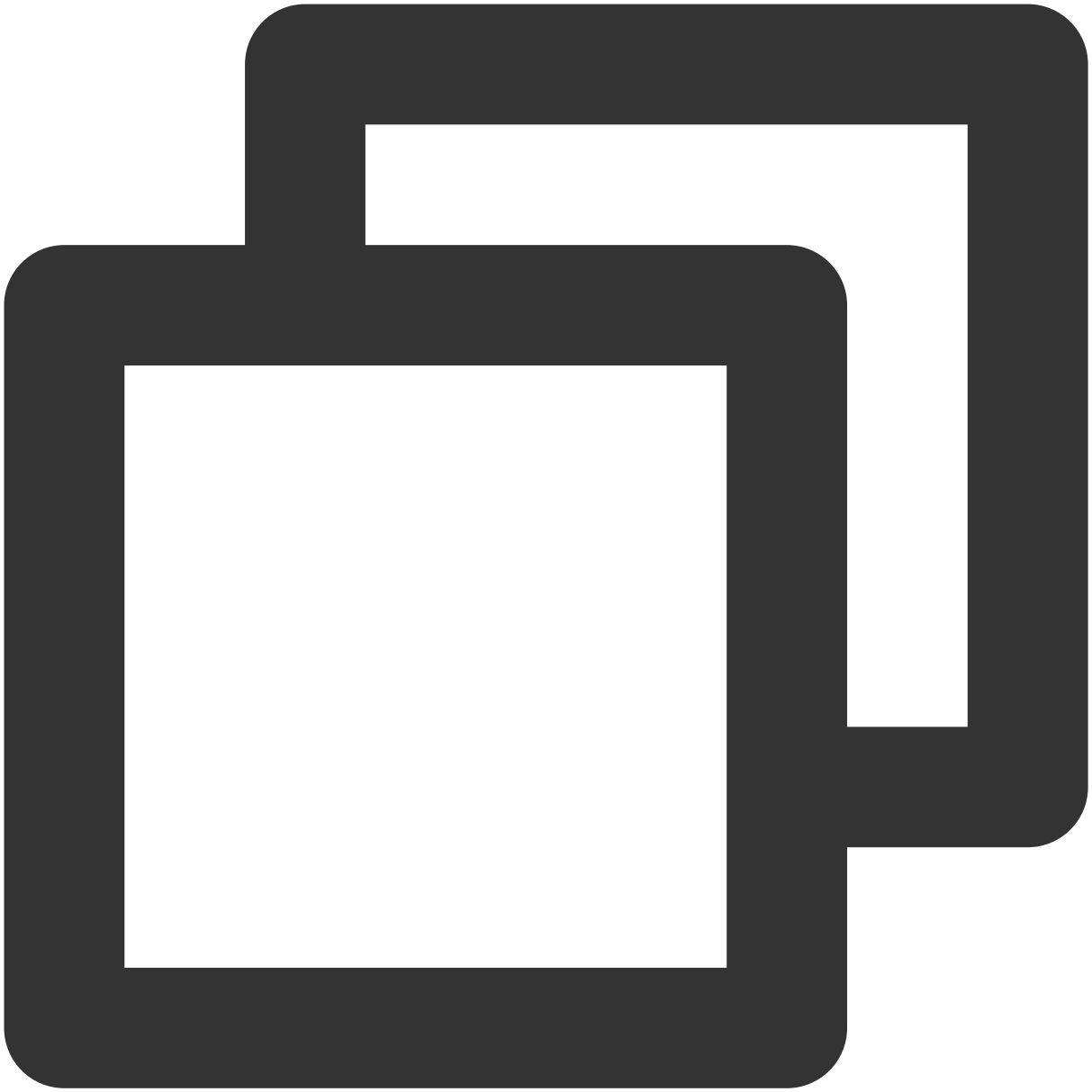
```
POST
```

请求路径



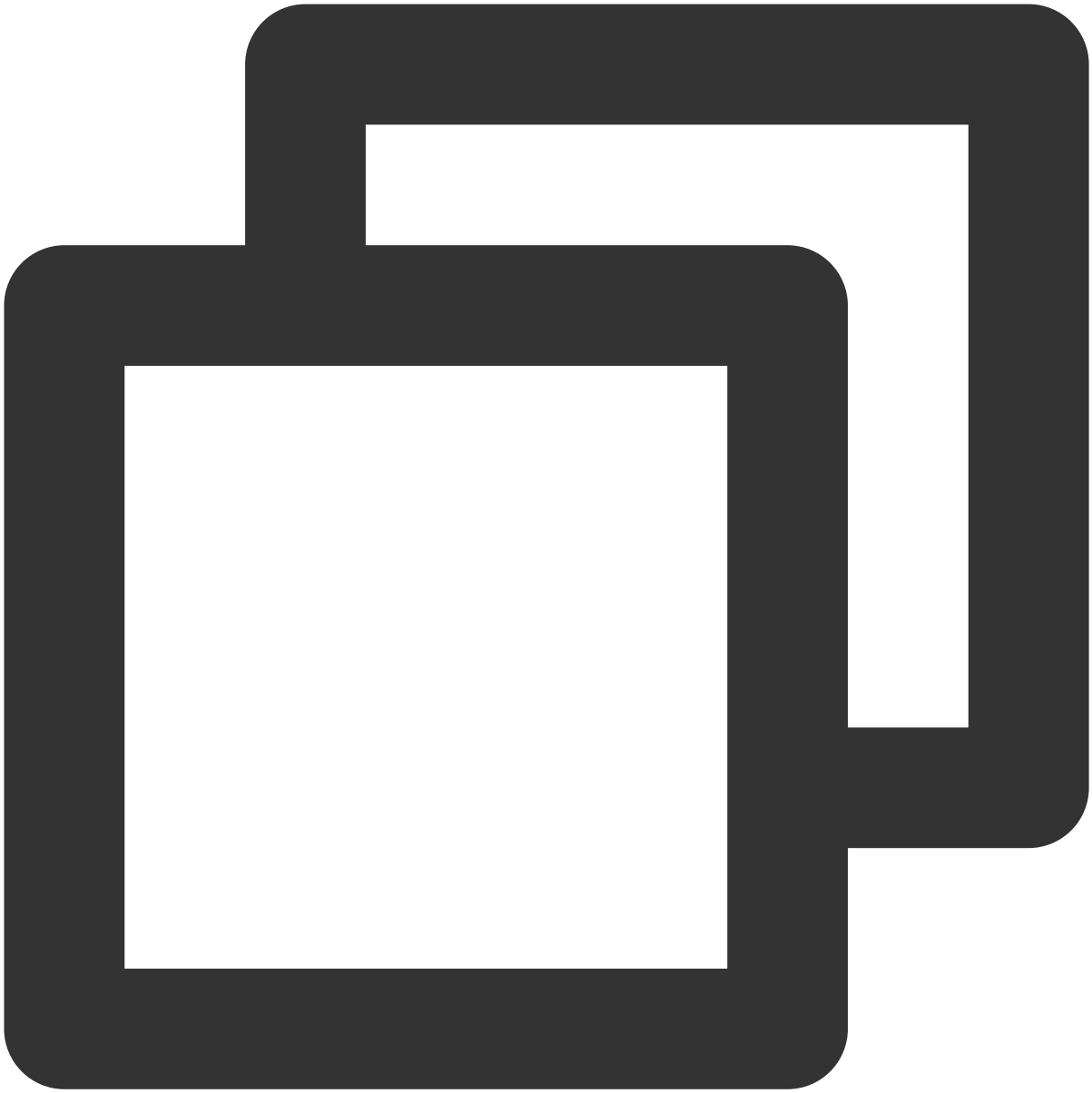
```
/oauth2/token
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例



```
POST /oauth2/token HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded
grant_type=password&client_id=TENANT_CLIENT_ID&client_secret=TENANT_CLIENT_SECRET&a
```

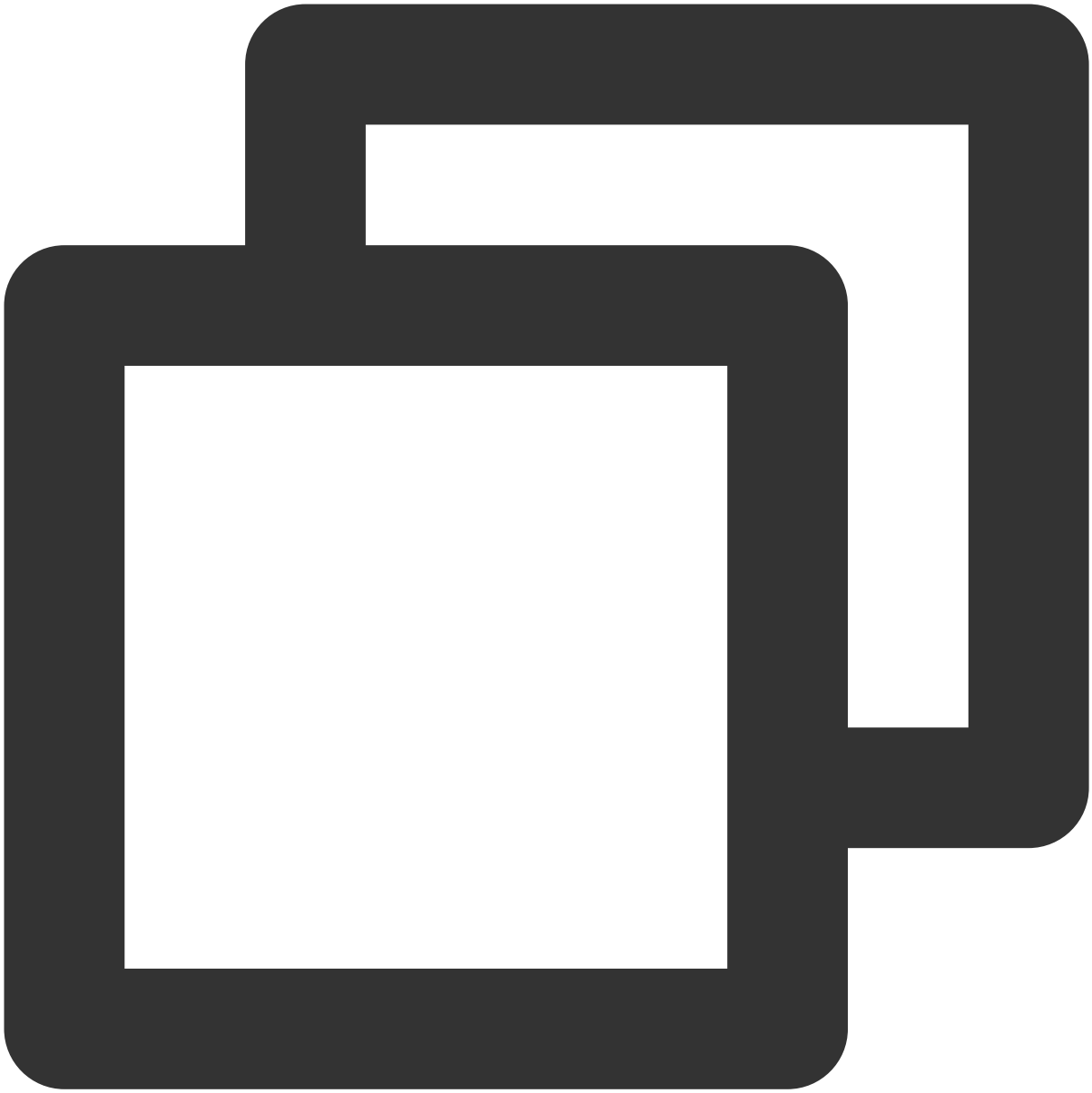
请求参数

参数	可选	描述

grant_type	false	填固定值 `password` 。
client_id	false	应用的 `client_id` 。可参考 **应用管理页面** > **选定指定应用** > 单击**应用配置** > 对应的“Client Id”。
client_secret	true	应用的 `client_secret` 。可参考 **应用管理页面** > **选定指定应用** > 单击**应用配置** > 对应的“client_secret”。 Web 应用须传递此参数。 单页应用和移动 App 不传递此参数。
auth_source_id	false	账号密码认证源 ID。可在控制台的 通用认证源页面 查看。
username	false	用户名。需要使用账号密码认证源配置的认证源属性，如用户名称、电话号码、邮箱地址。
password	false	用户密码。
scope	true	可省略。如传递，则填固定值 `openid` 。

正常响应示例

认证成功



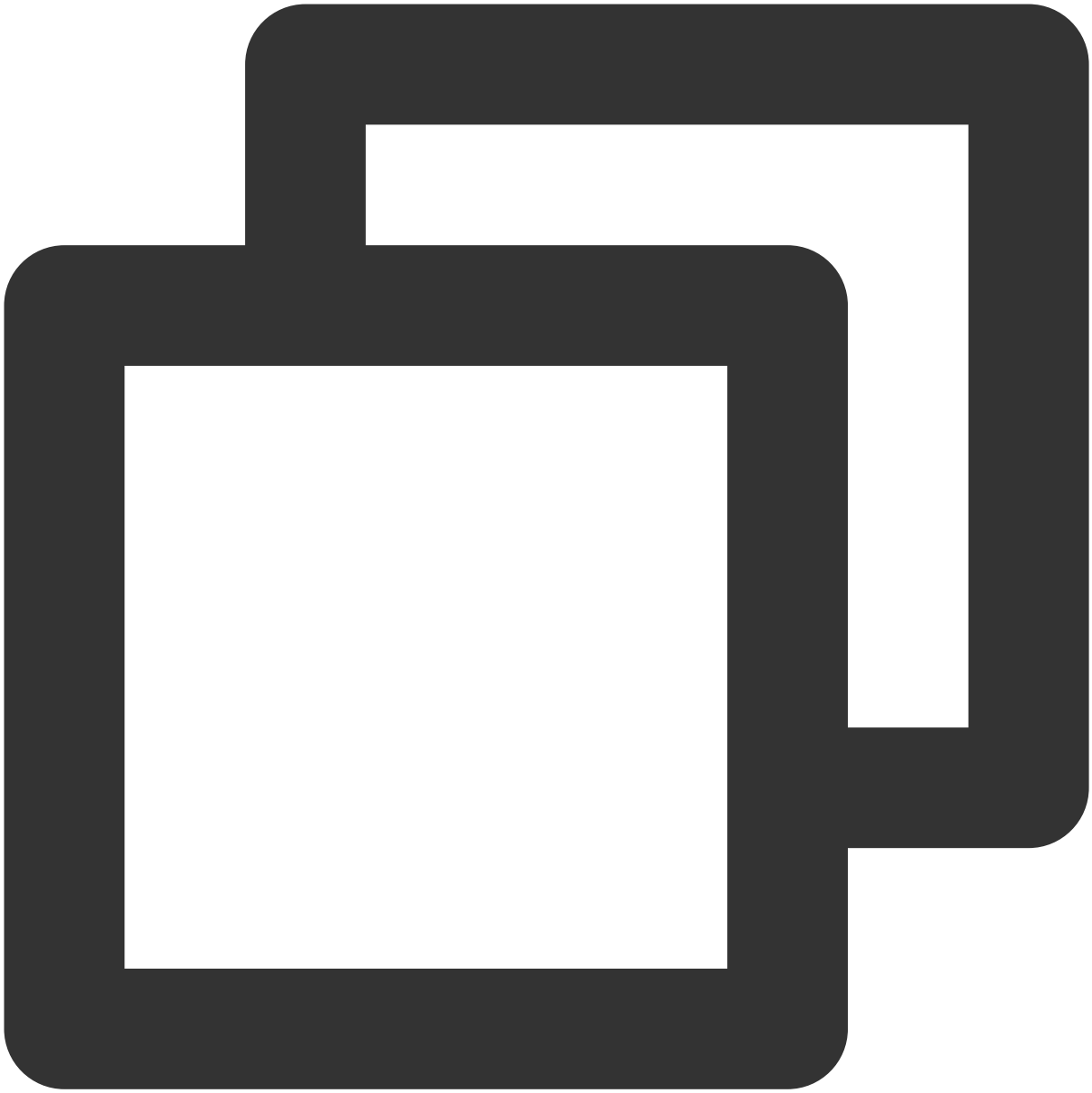
```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiI1MzQyOGU3ZS1kOTJiLTQ3OTAtOGIwMC0wMmEyZjc4NjUxNzMiLCJ
  "refresh_token" : "7uqTlthTQrzIZx8joT20chQbakZp81_iv39GTyCpsEyYpWoquNhuB3s6qEQHGe
  "scope" : "openid",
  "id_token" : "eyJraWQiOiI1MzQyOGU3ZS1kOTJiLTQ3OTAtOGIwMC0wMmEyZjc4NjUxNzMiLCJ0eXA
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

响应参数

参数	数据类型	描述
access_token	String	OAuth 2.0 Access Token (JWT)。
token_type	String	Token 类型，目前返回的是固定值 `Bearer` 。
expires_in	Number	Access Token 有效期，单位秒。
scope	String	Access Token scope。
refresh_token	String	OAuth 2.0 Refresh Token。
id_token	String	OIDC ID Token (JWT)。

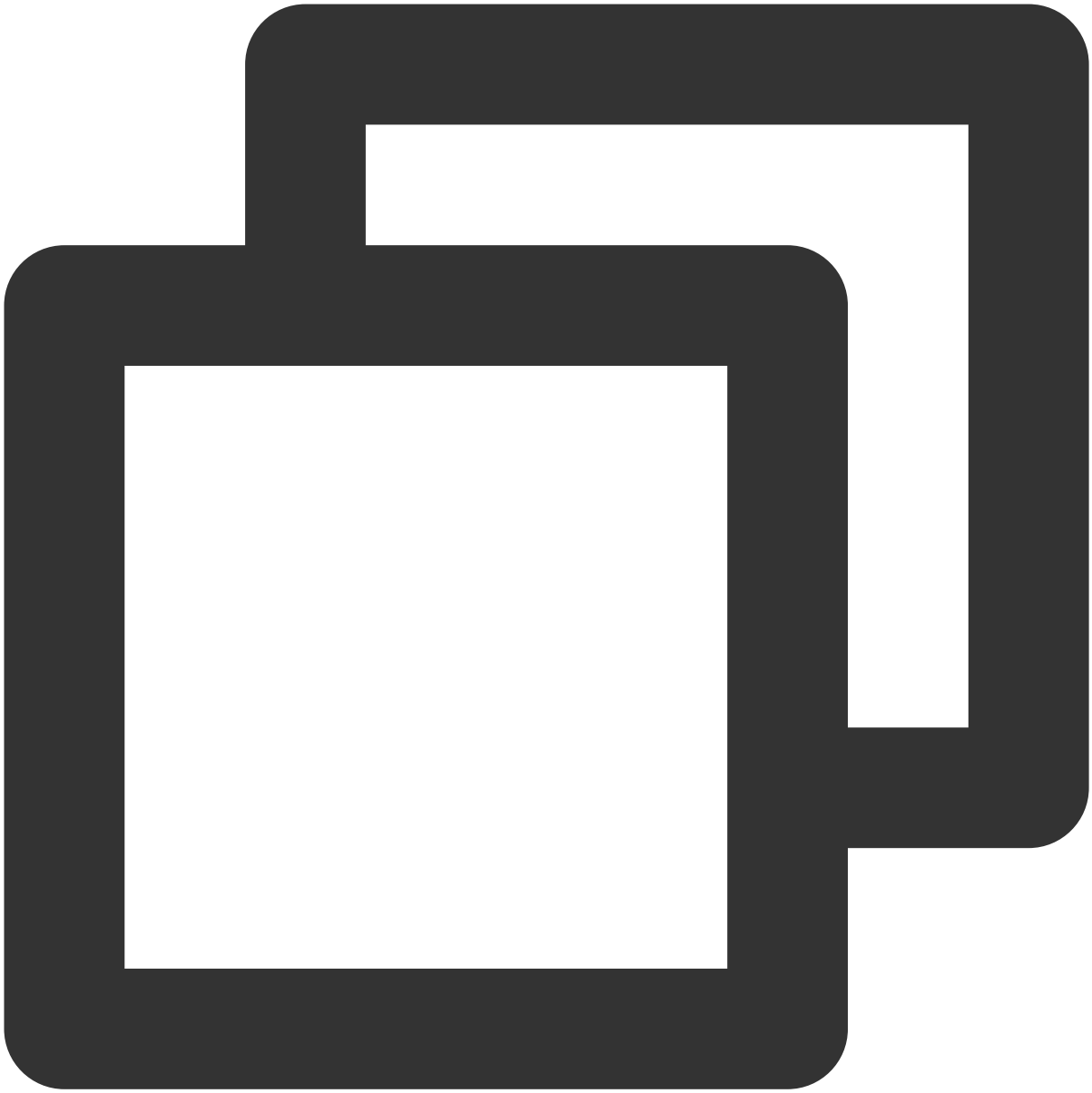
异常响应示例

用户名密码错误。



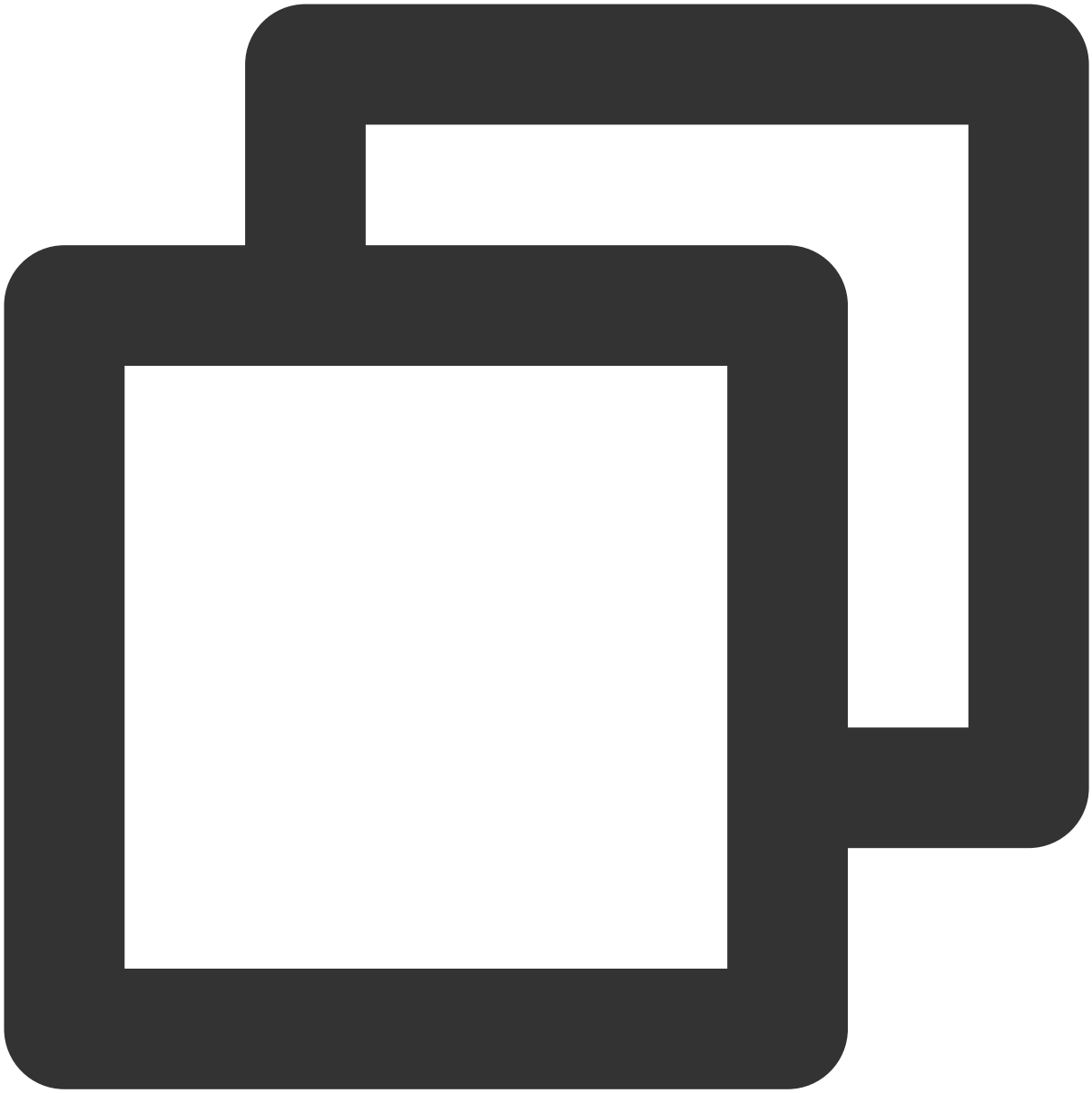
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Wrong username or password"
}
```

用户状态异常（如被锁定或冻结）。



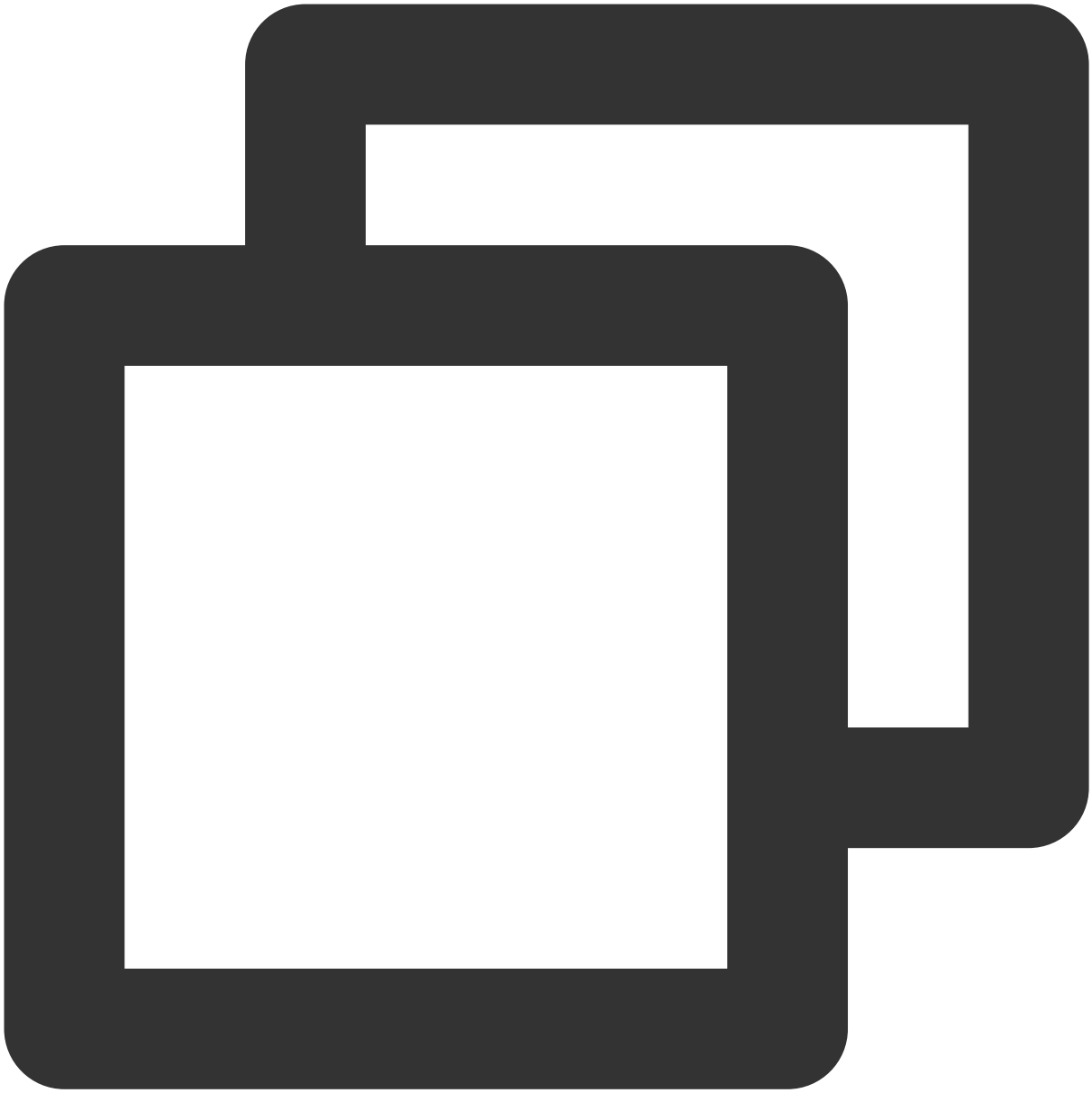
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Abnormal user status"
}
```

使用了认证源不支持的属性作为用户名（例如：username 传入了邮箱地址，但账号密码认证源未配置邮箱地址为认证源属性）。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Unsupported username identifier"
}
```

认证源不是应用的首选认证源或关联认证源。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_auth_source",
"error_description" : "Auth source and application not associated"
}
```

短信和邮箱 OTP 认证

最近更新时间：2023-12-22 11:42:07

接口描述

校验短信或邮箱 OTP 验证码，获取 Access Token 和 ID Token，完成登录。调用此接口前，需要先通过 发送 OTP 验证码 接口向用户发送验证码。

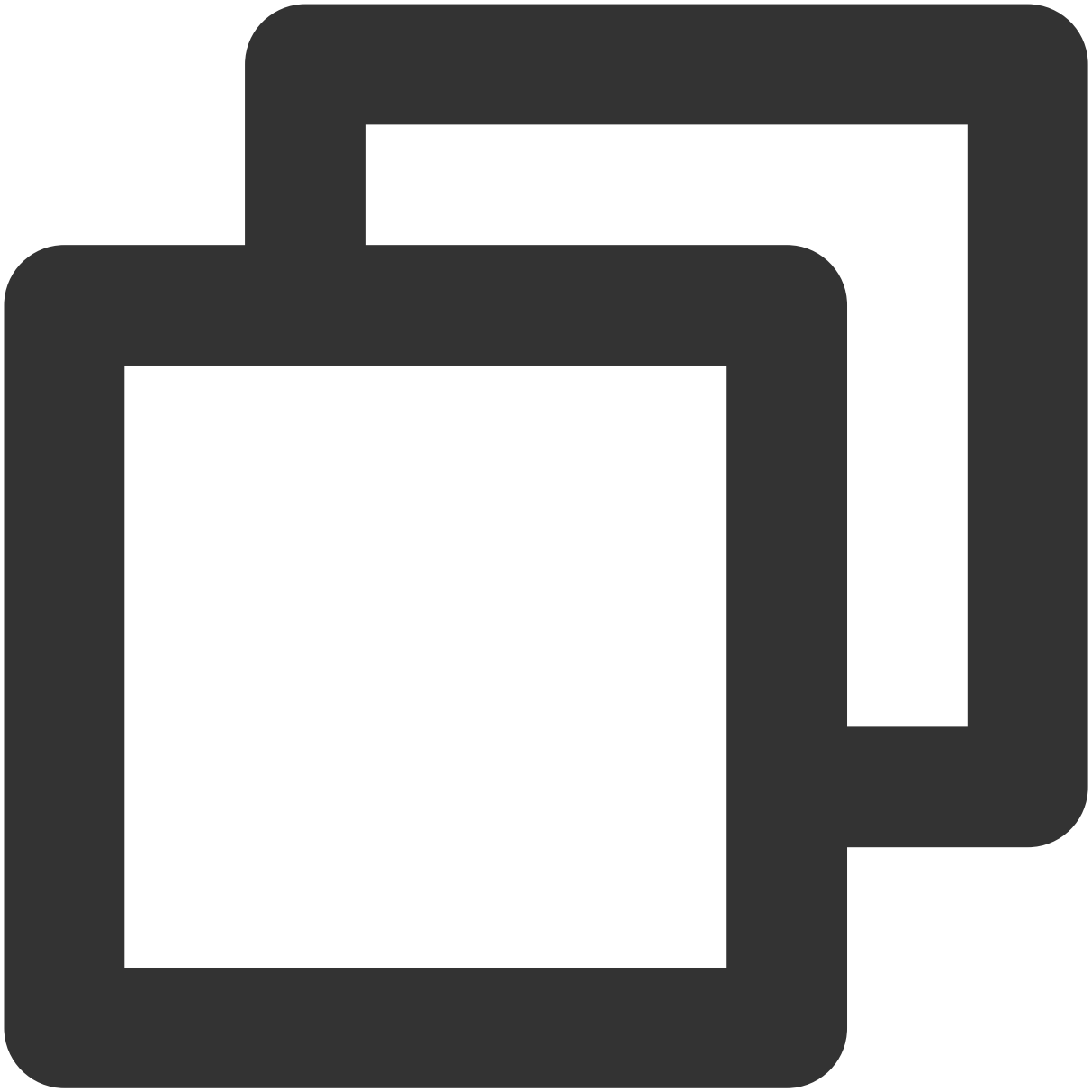
说明：

可以通过传递 `auto_signup=true` 参数来支持自动注册用户。

支持的应用类型

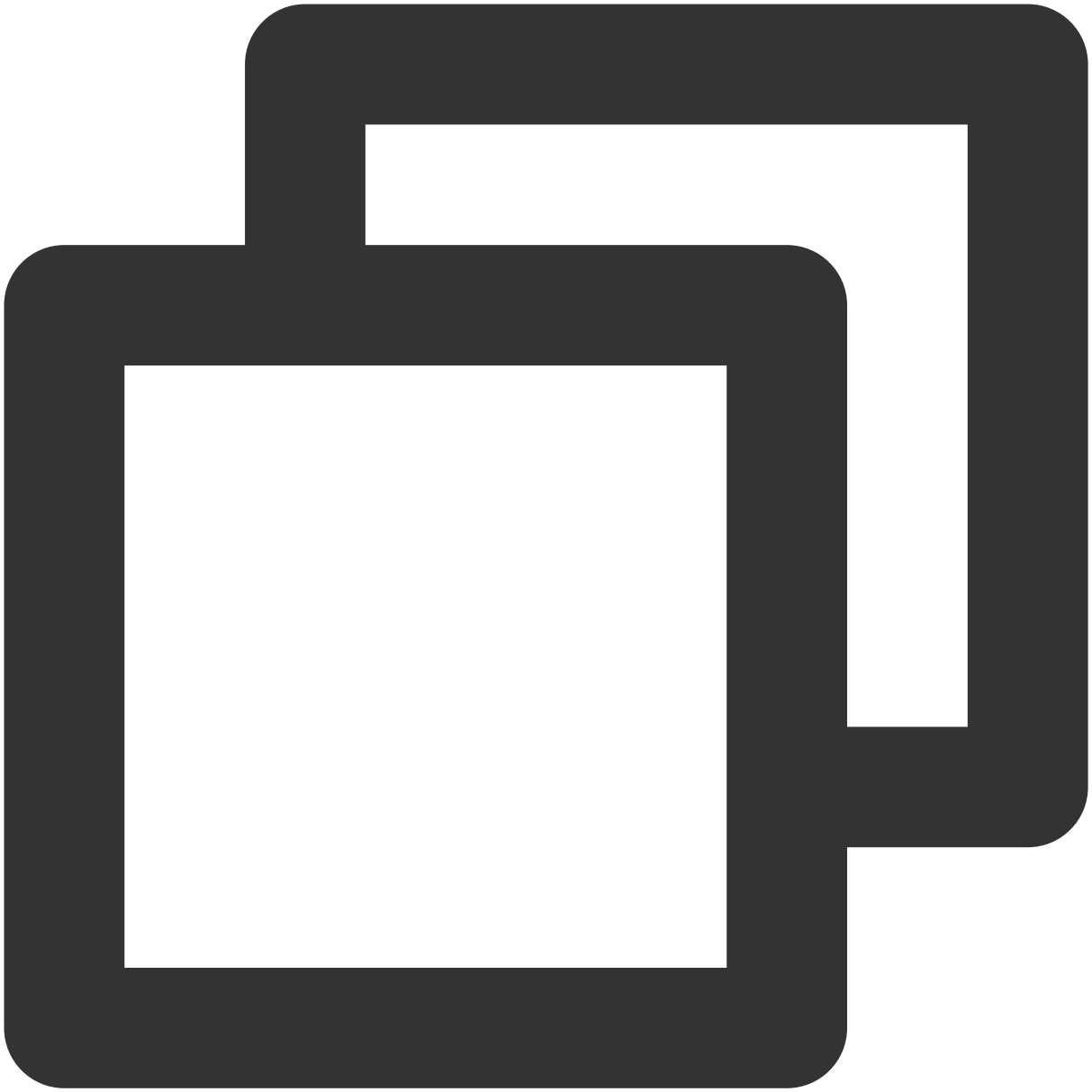
Web 应用、单页应用、移动 App。

请求方法



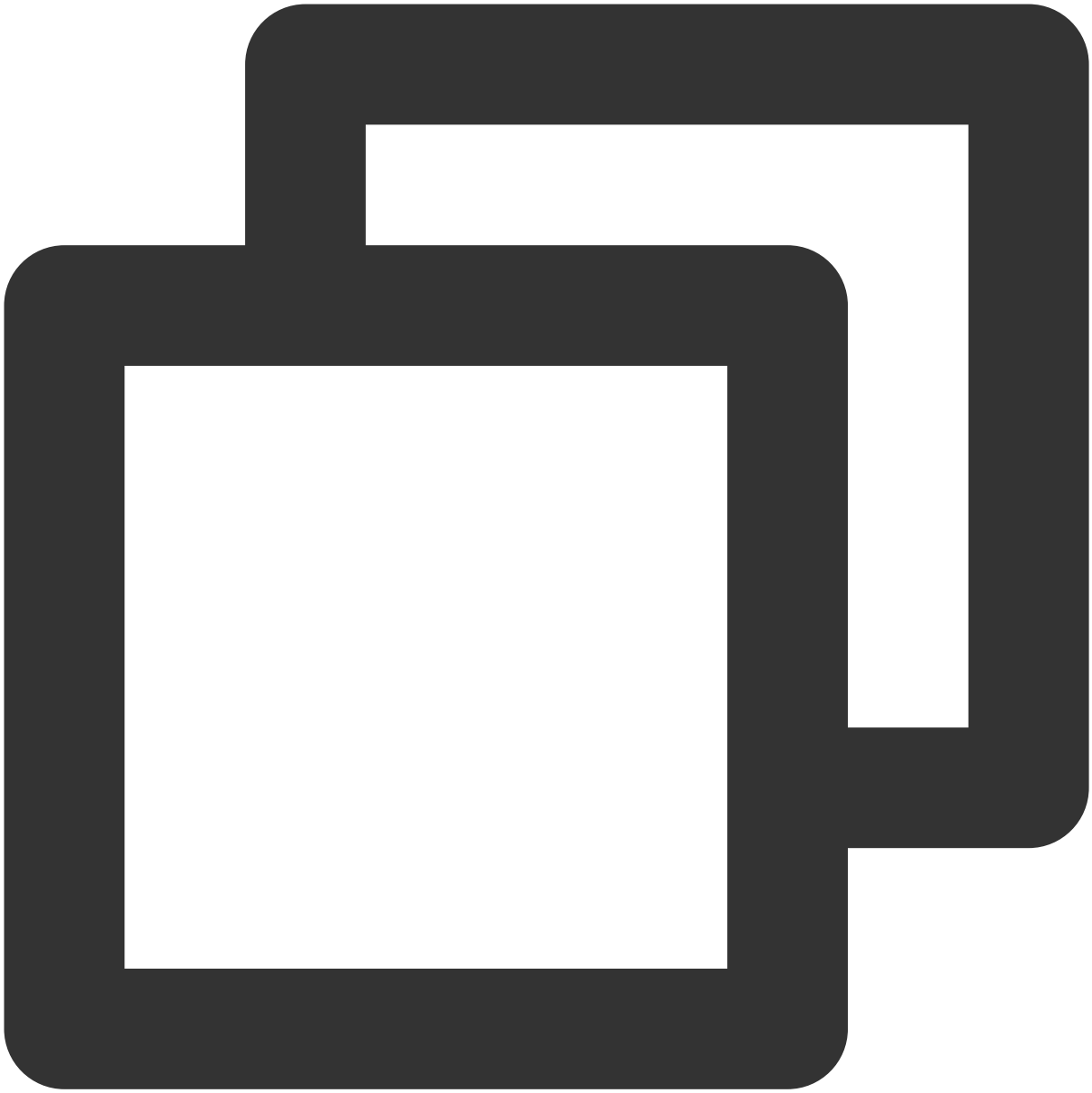
```
POST
```

请求路径



```
/oauth2/token
```

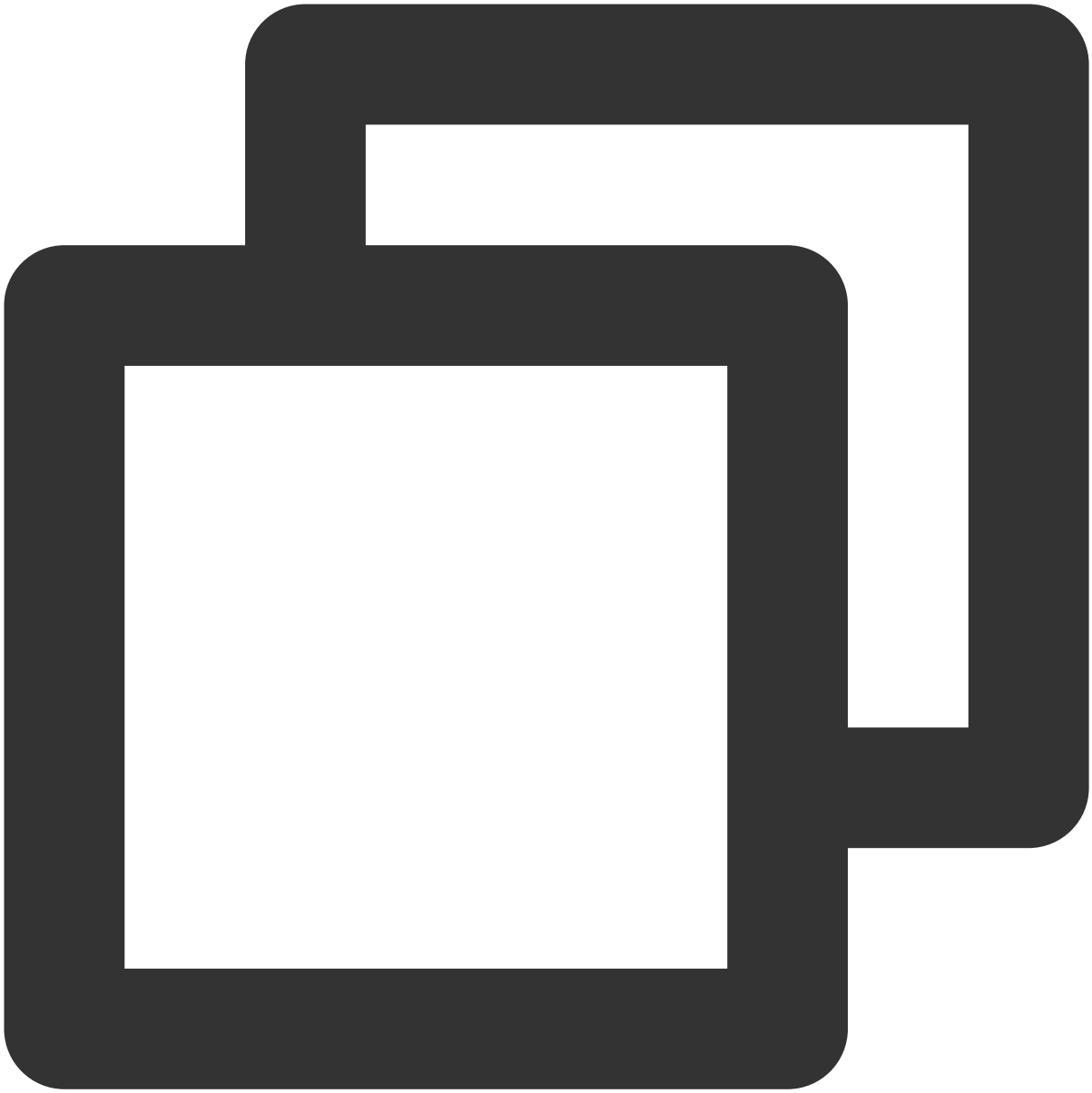
请求 Content-Type



```
application/json
```

请求示例

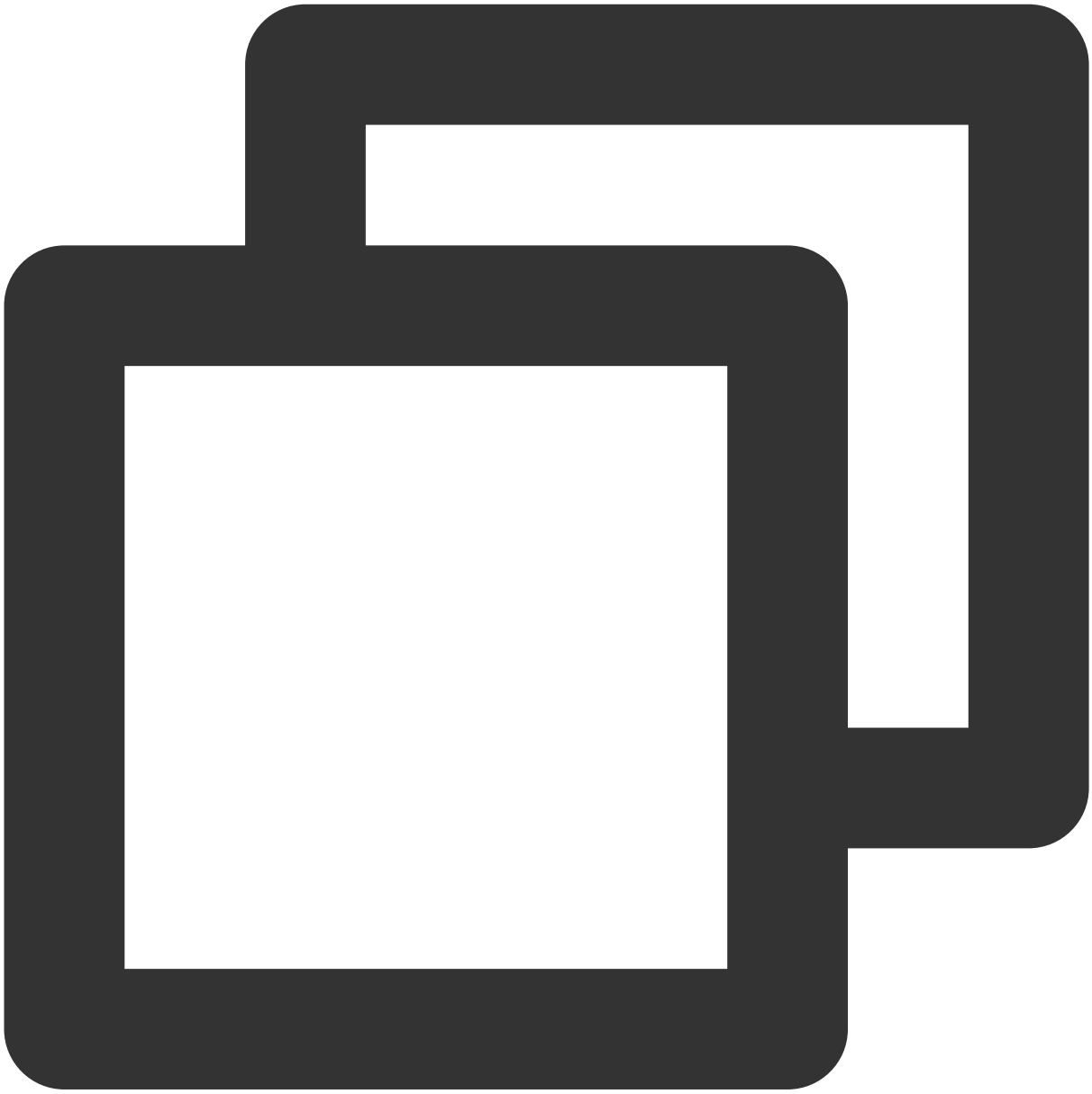
短信 OTP 登录



```
POST /oauth2/token HTTP/1.1
Content-Type: application/json
Host: sample.portal.tencentciam.com

{
  "grant_type" : "http://tencentciam.com/oauth2/grant-type/otp/sms",
  "client_id" : "TENANT_CLIENT_ID",
  "client_secret" : "TENANT_CLIENT_SECRET",
  "auth_source_id" : "MOCK_SMS_OTP_AUTH_SOURCE_ID",
  "phone_number" : "13612345678",
  "otp_token" : "MOCK_OTP_TOKEN",
```

```
  "otp" : "123456"
}
```

邮箱 OTP 登录



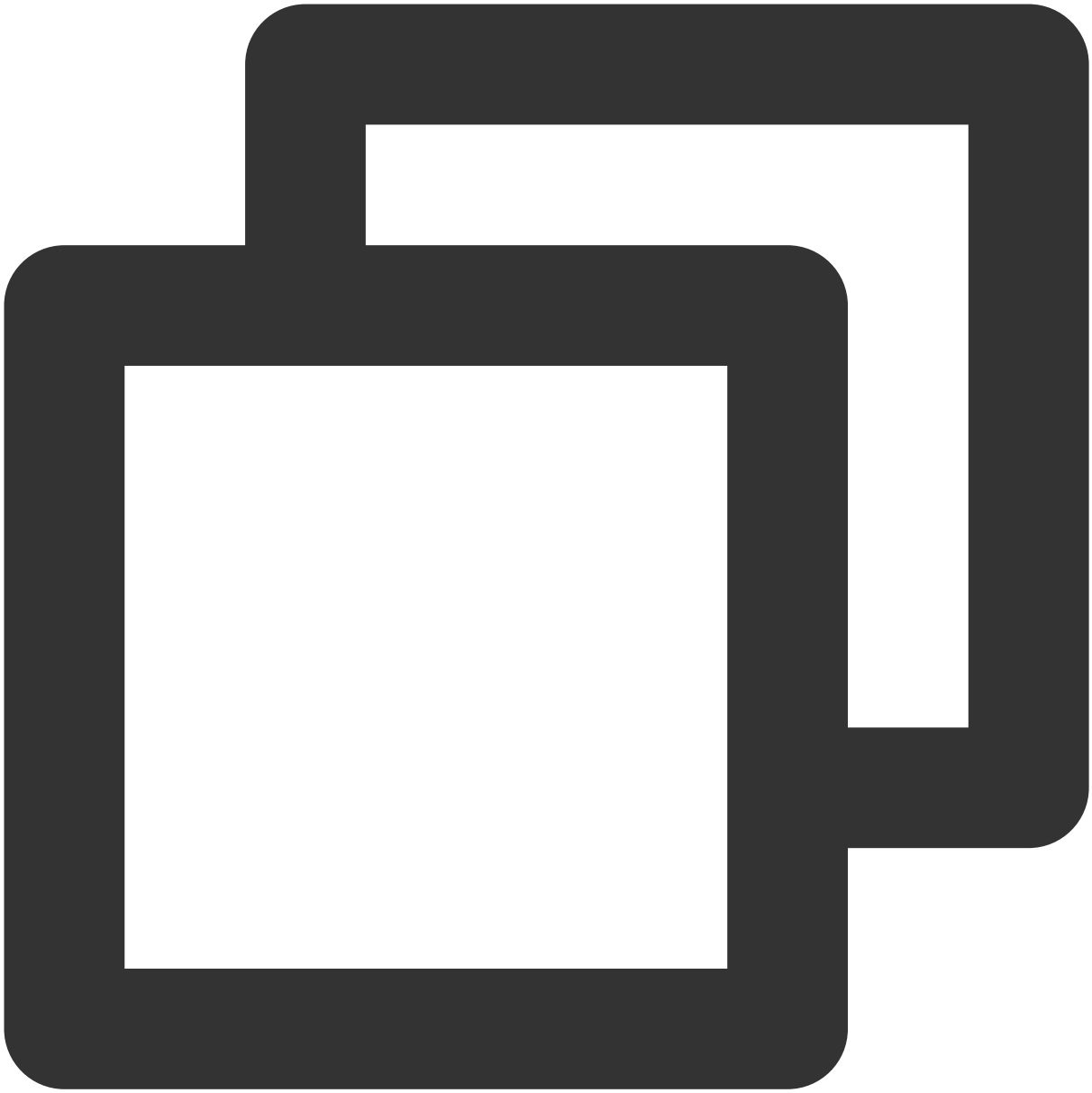
```
POST /oauth2/token HTTP/1.1
Content-Type: application/json
Host: sample.portal.tencentciam.com

{
  "grant_type" : "http://tencentciam.com/oauth2/grant-type/otp/email",
```

```
  "client_id" : "TENANT_CLIENT_ID",
  "client_secret" : "TENANT_CLIENT_SECRET",
  "auth_source_id" : "MOCK_EMAIL_OTP_AUTH_SOURCE_ID",
  "email" : "MOCK_USERNAME@example.com",
  "otp_token" : "MOCK_EMAIL_OTP_TOKEN",
  "otp" : "123456"
}
```

请求体 JSON 参数

JSON 路径	数据类型	描述
grant_type	String	短信 OTP 登录输入：`http://tencentciam.com/oauth2/grant-type/otp/sms` 邮箱 OTP 登录输入：`http://tencentciam.com/oauth2/grant-type/otp/email`
client_id	String	应用的 `client_id` 。需要与发送验证码时使用的一致。
client_secret	String	应用的 `client_secret` 。Web 应用须传递此参数。单页应用和移动 App 不传递此参数。
auth_source_id	String	短信 OTP 或邮箱 OTP 认证源 ID。需要与发送验证码时使用的一致。
phone_number	String	用户的手机号。需要与发送验证码时使用的一致。短信 OTP 登录时传递此参数。
email	String	用户的邮箱地址。需要与发送验证码时使用的一致。邮箱 OTP 登录时传递此参数。
otp_token	String	发送验证码成功后服务端返回的 `otp_token` 。
otp	String	用户手机或邮箱收到的 OTP 验证码。
auto_signup	Boolean	如需支持自动注册用户，则此参数传 true，否则可以不传。

正常响应示例



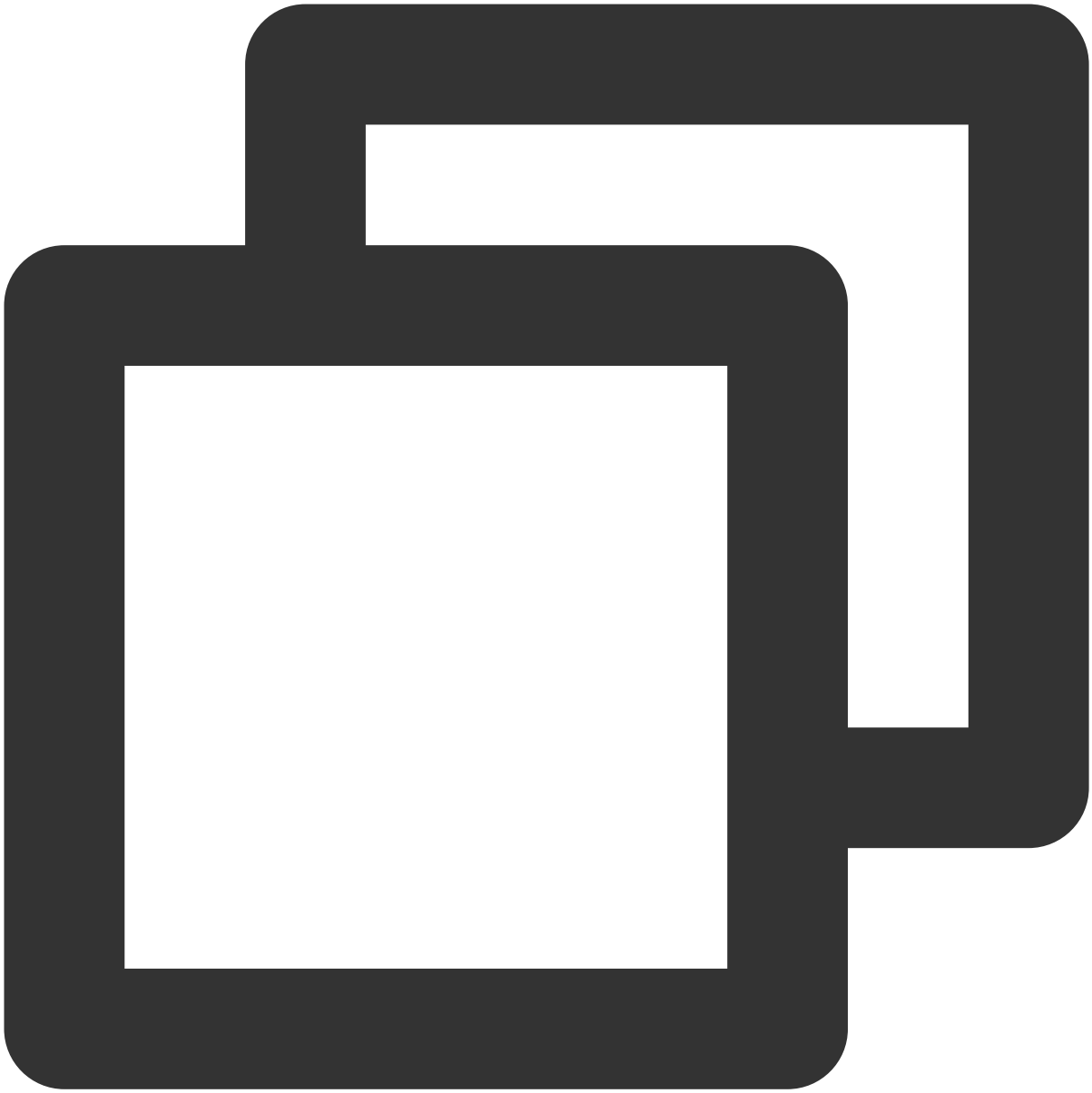
```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiJmZTQ4YTJjYS1lNGU3LTQyMGEtOThjOS01OGM5NmI2NzUwZjIiLCJ
  "refresh_token" : "B-72VlkQa3jQNuo9Xbbl-muoh4w7nYu-7Q3Wb-qmPgyftN1CgXPov2aWsOBWee
  "scope" : "openid",
  "id_token" : "eyJraWQiOiJmZTQ4YTJjYS1lNGU3LTQyMGEtOThjOS01OGM5NmI2NzUwZjIiLCJ0eXA
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

响应参数

字段	数据类型	描述
access_token	String	OAuth 2.0 Access Token (JWT)。
token_type	String	Token 类型，目前返回的是固定值 'Bearer'。
expires_in	Number	Access Token 有效期，单位秒。
scope	String	Access Token scope。
refresh_token	String	OAuth 2.0 Refresh Token。
id_token	String	OIDC ID Token (JWT)。

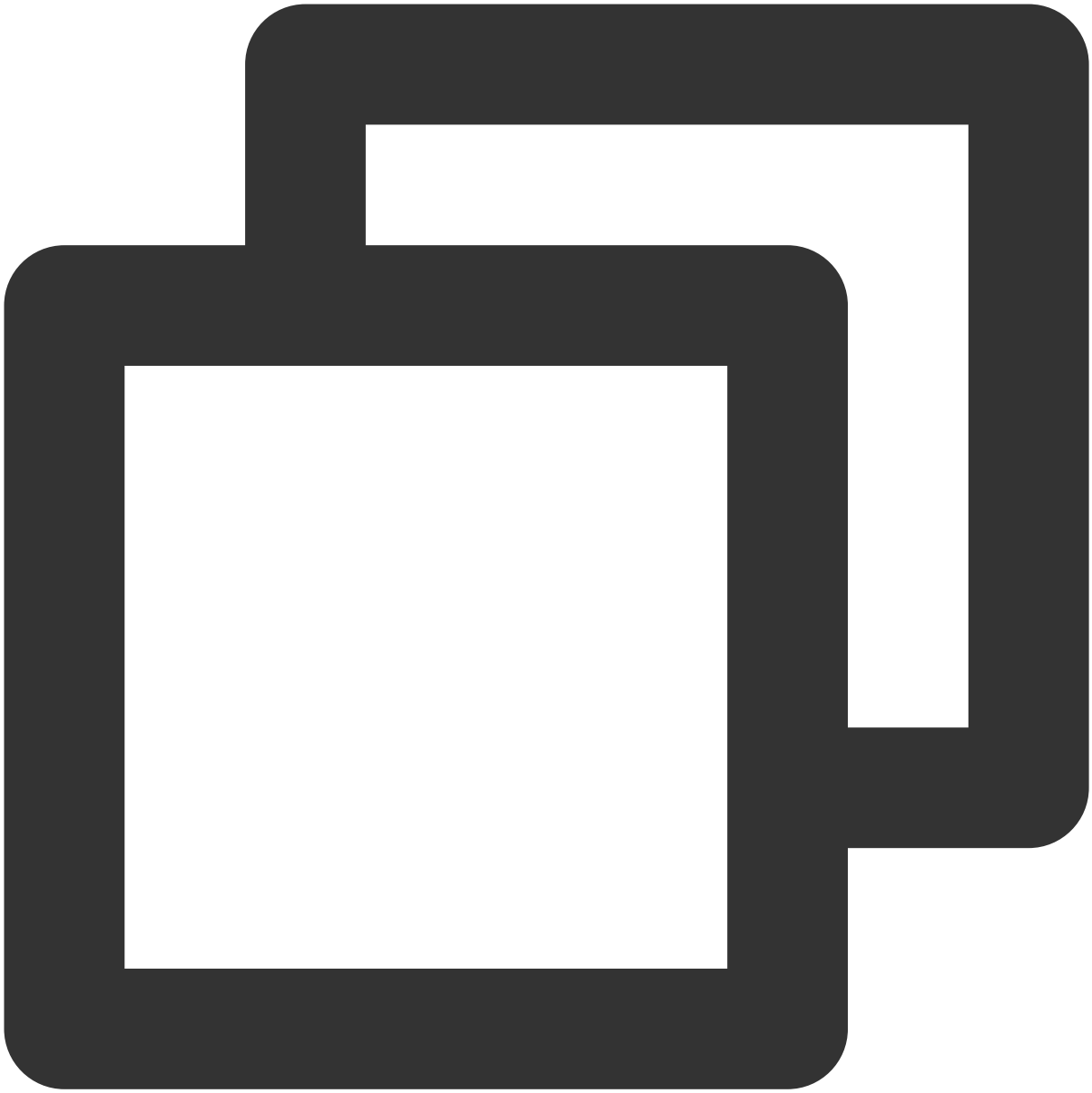
异常响应示例

otp_token 错误或已过期。



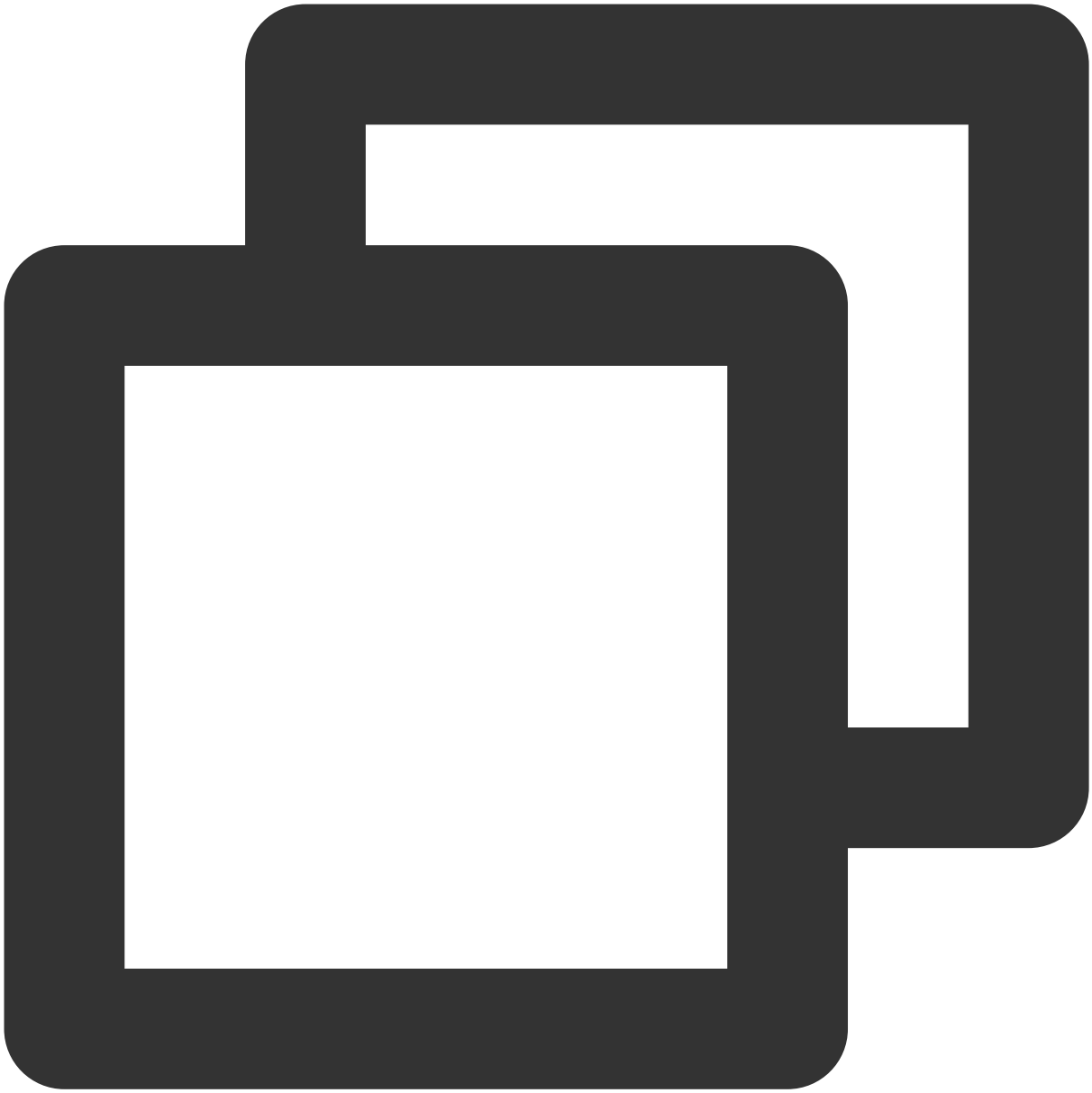
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Unknown or expired otp_token"
}
```

otp 错误或已过期。



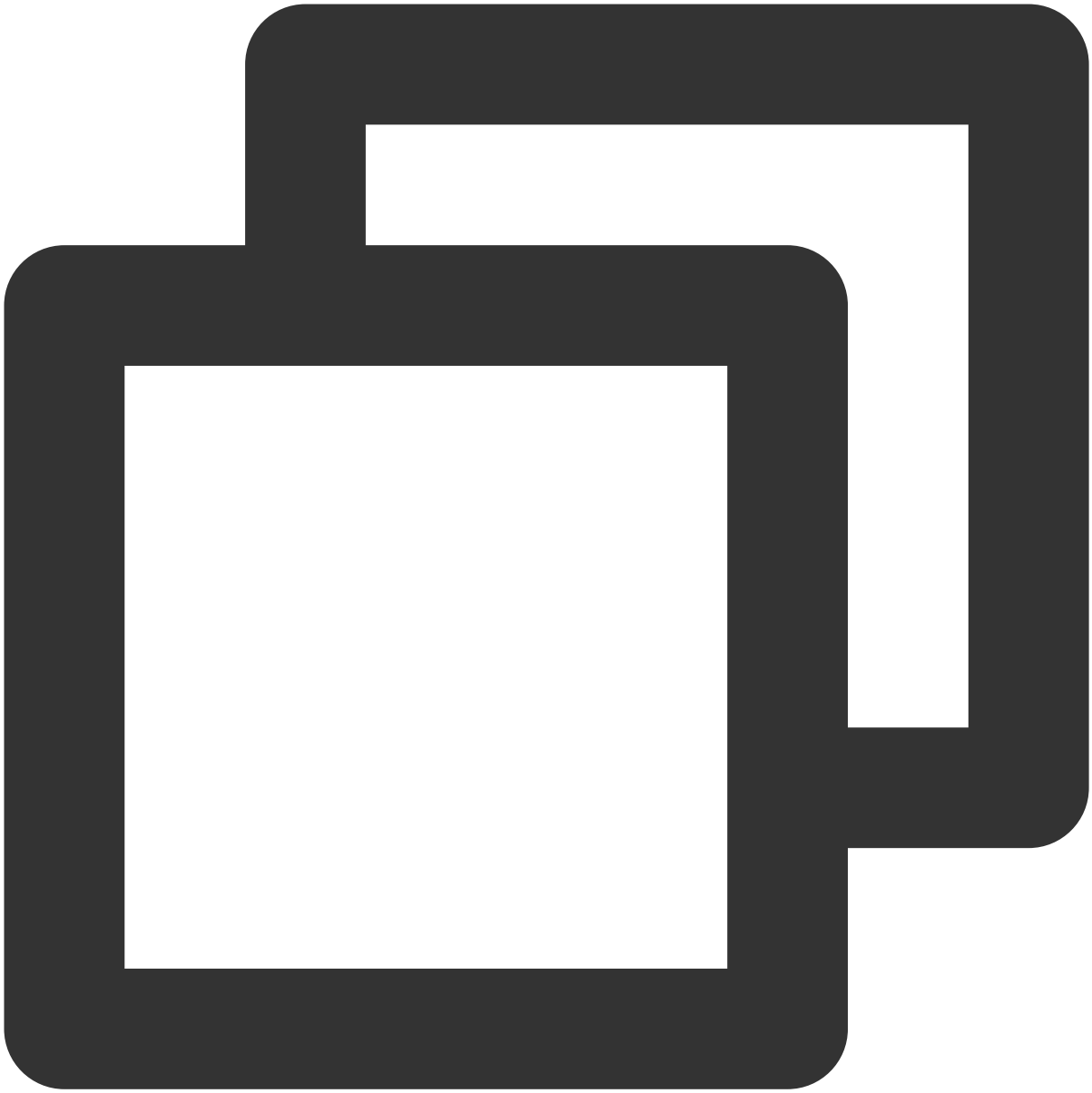
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Unknown or expired OTP"
}
```

使用的参数与发送验证码时不一致（例如：手机号不同）。



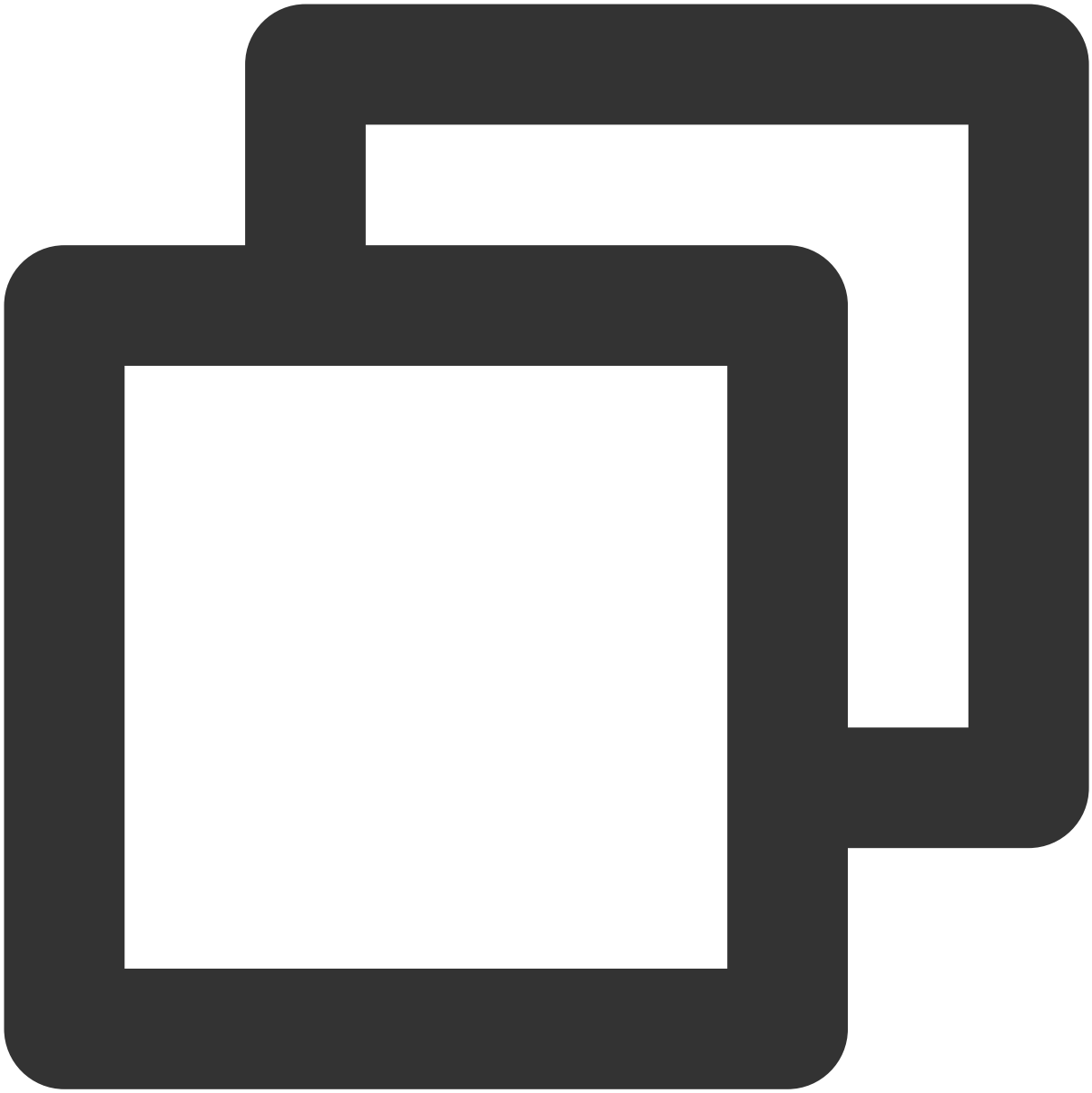
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_request",
"error_description" : "Mismatched OTP token and OTP sending parameters"
}
```

找不到手机号或邮箱对应的用户（不允许自动注册用户的情况下）。



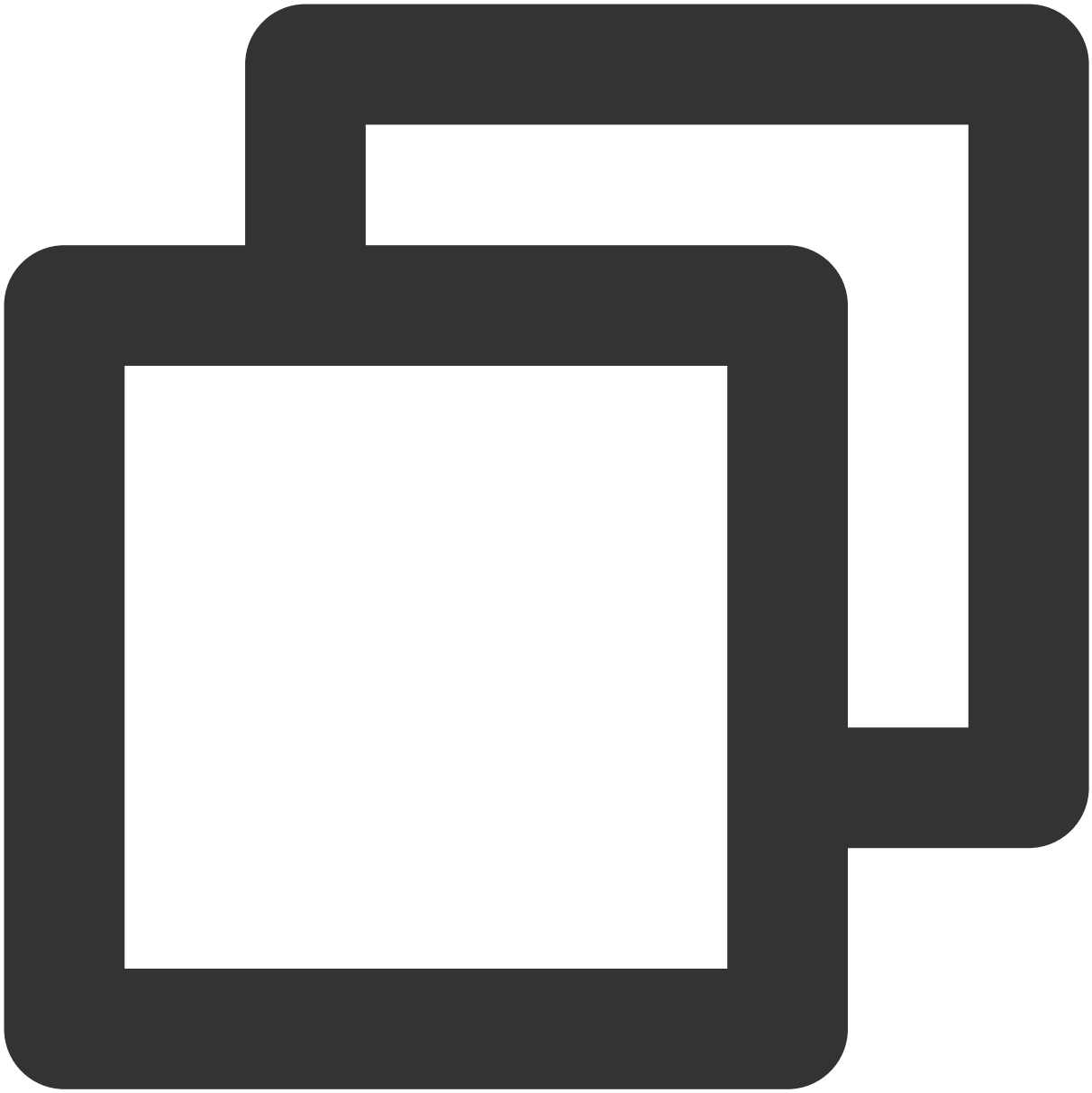
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "User not found"
}
```

手机号或邮箱对应的用户状态异常（如被锁定或冻结）。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant",
"error_description" : "Abnormal user status"
}
```

认证源不是应用的首选认证源或关联认证源。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_auth_source",
"error_description" : "Auth source and application not associated"
}
```

发送 OTP 验证码

最近更新时间：2023-12-22 11:42:08

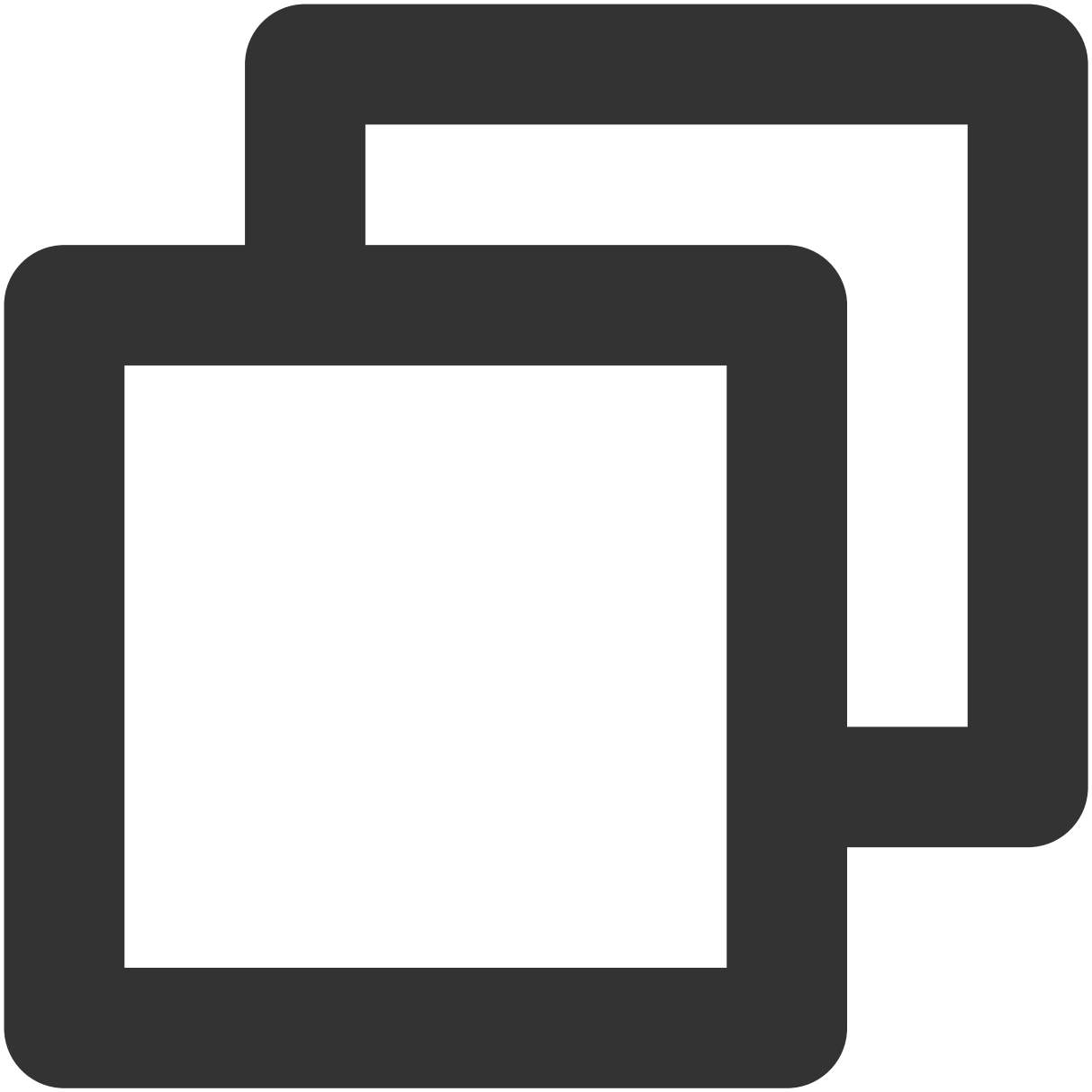
接口描述

向用户发送短信或邮箱 OTP 验证码，用于登录、注册或更新用户信息。

支持的应用类型

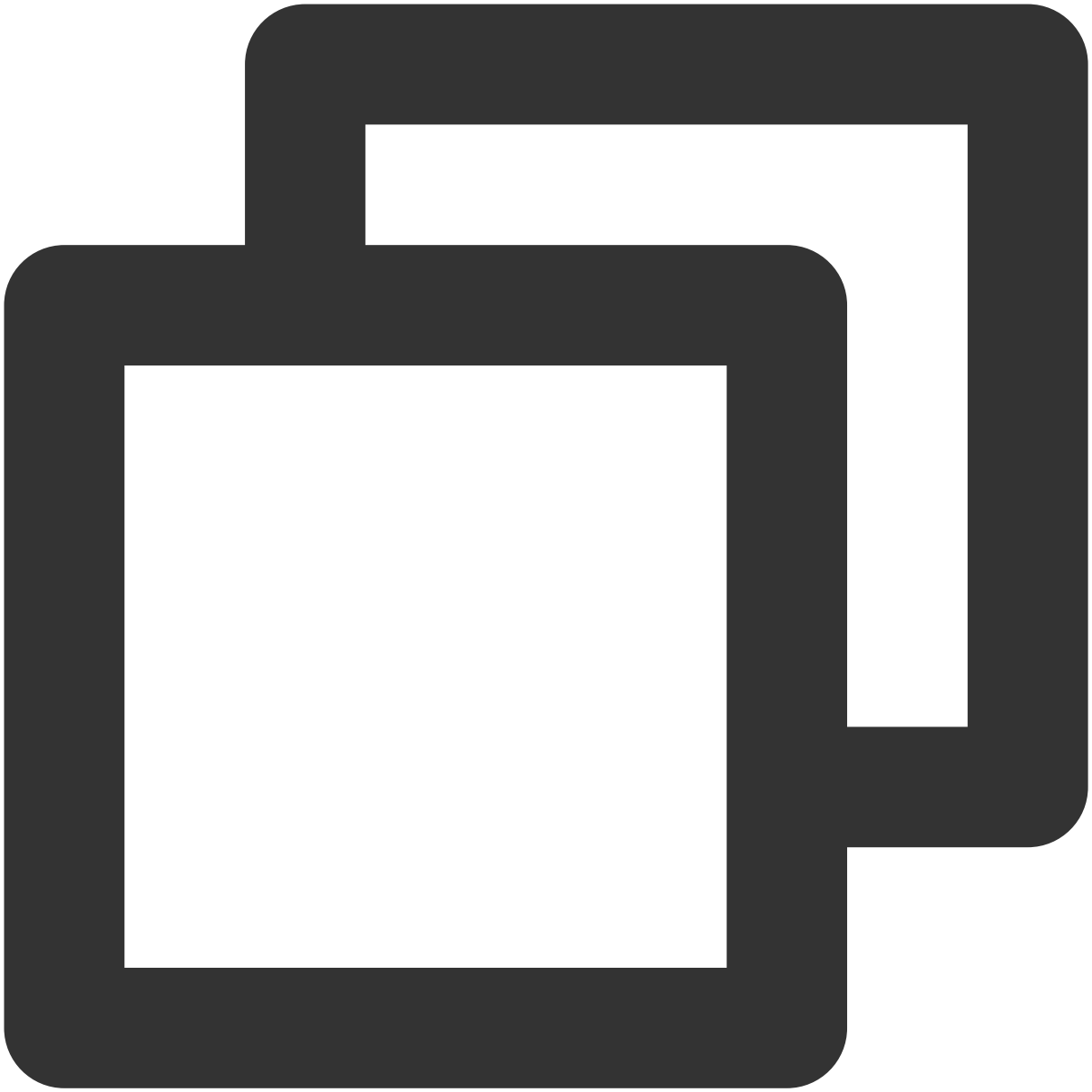
Web 应用、M2M 应用。

请求方法



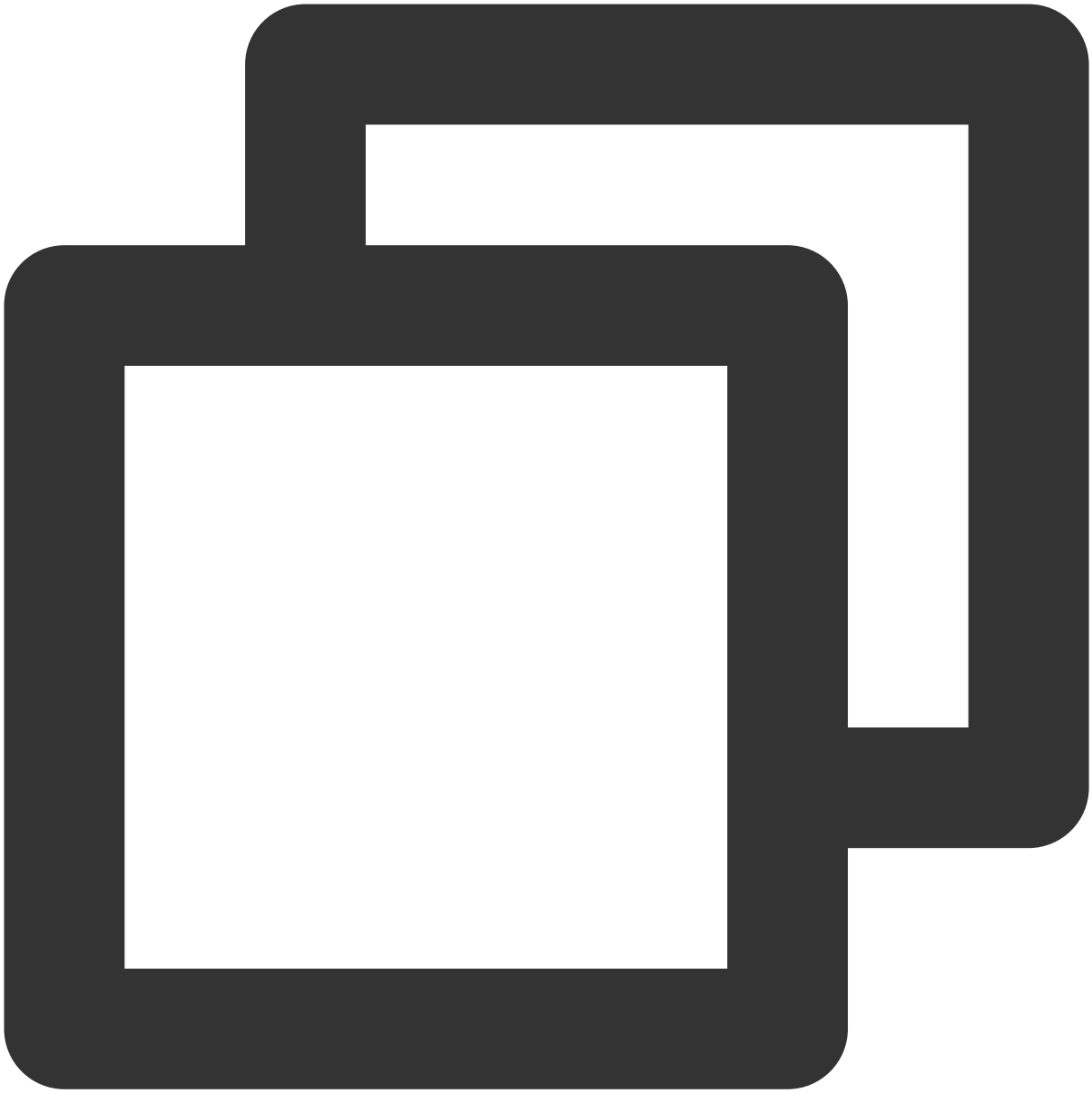
```
POST
```

请求路径



```
/otp/send
```

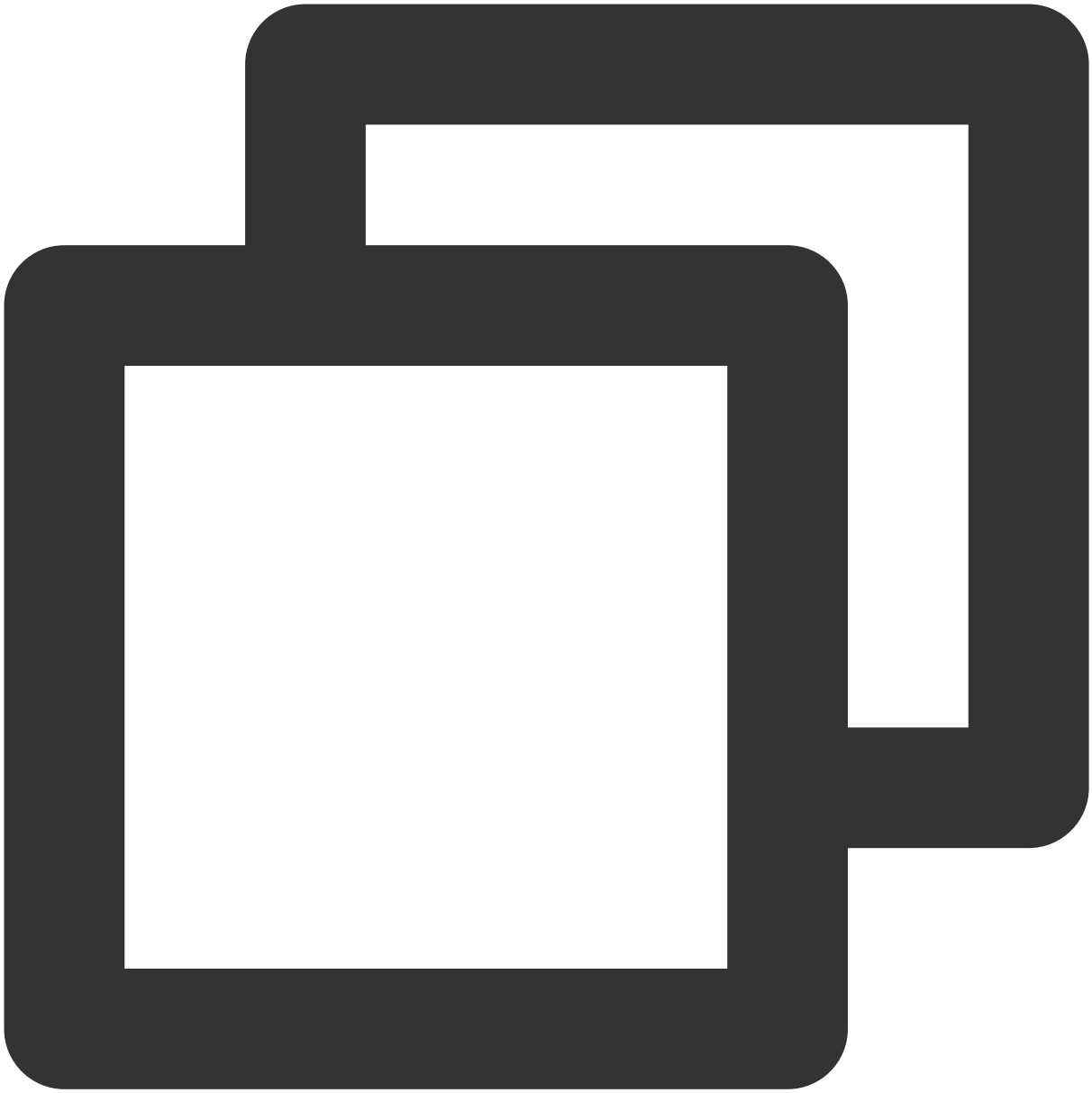
请求 Content-Type



```
application/json
```

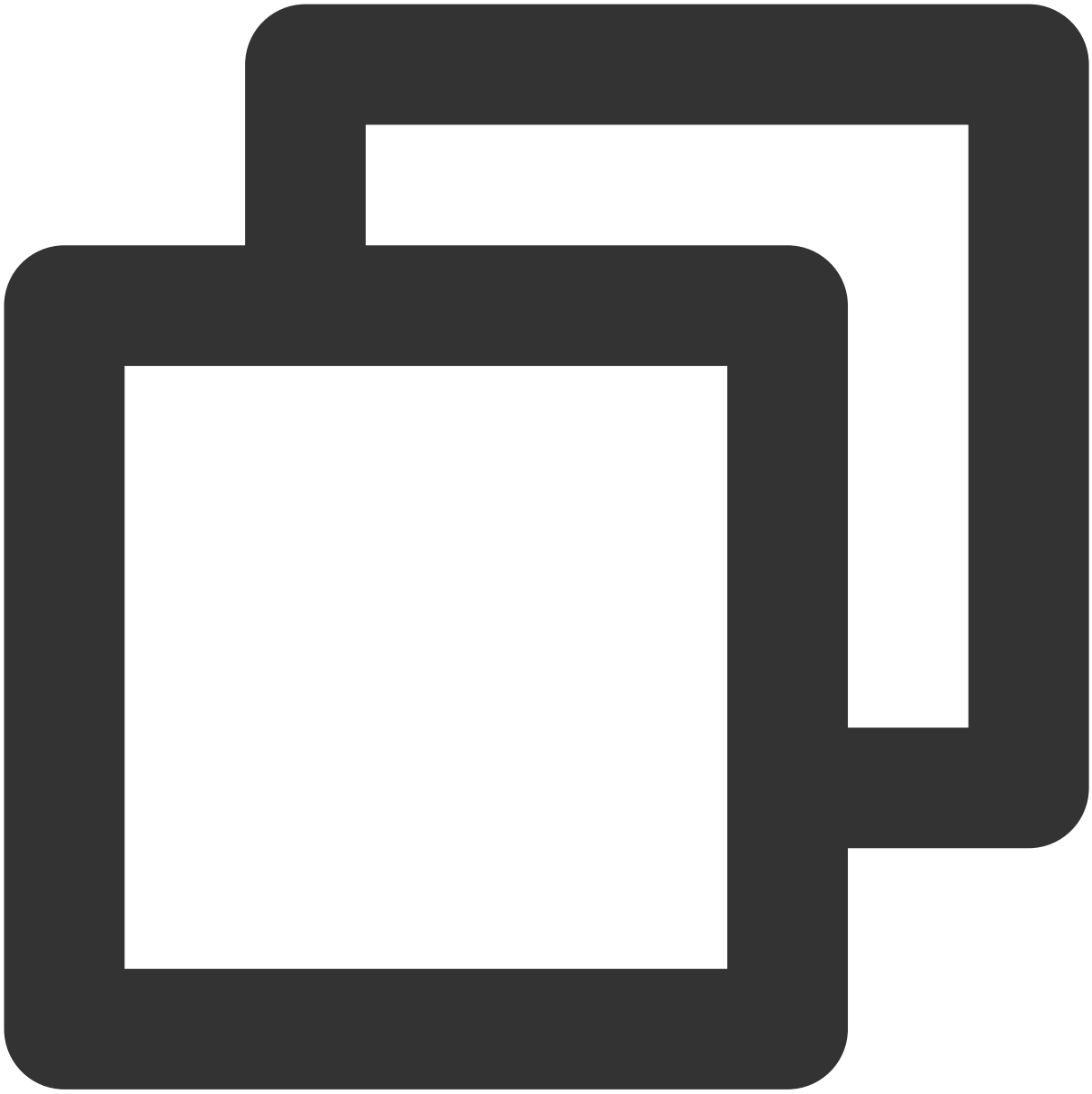
请求示例

短信 OTP 登录场景，发送短信验证码用于登录。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic VEVOQU5UX0NMSUVOVF9JRDpURU5BTlRfQ0xJRU5UX1NFQ1JFVA==
Host: sample.portal.tencentciam.com

{
"usage" : "login",
"phone_number" : "13612345678",
"auth_source_id" : "MOCK_SMS_OTP_AUTH_SOURCE_ID"
}
```

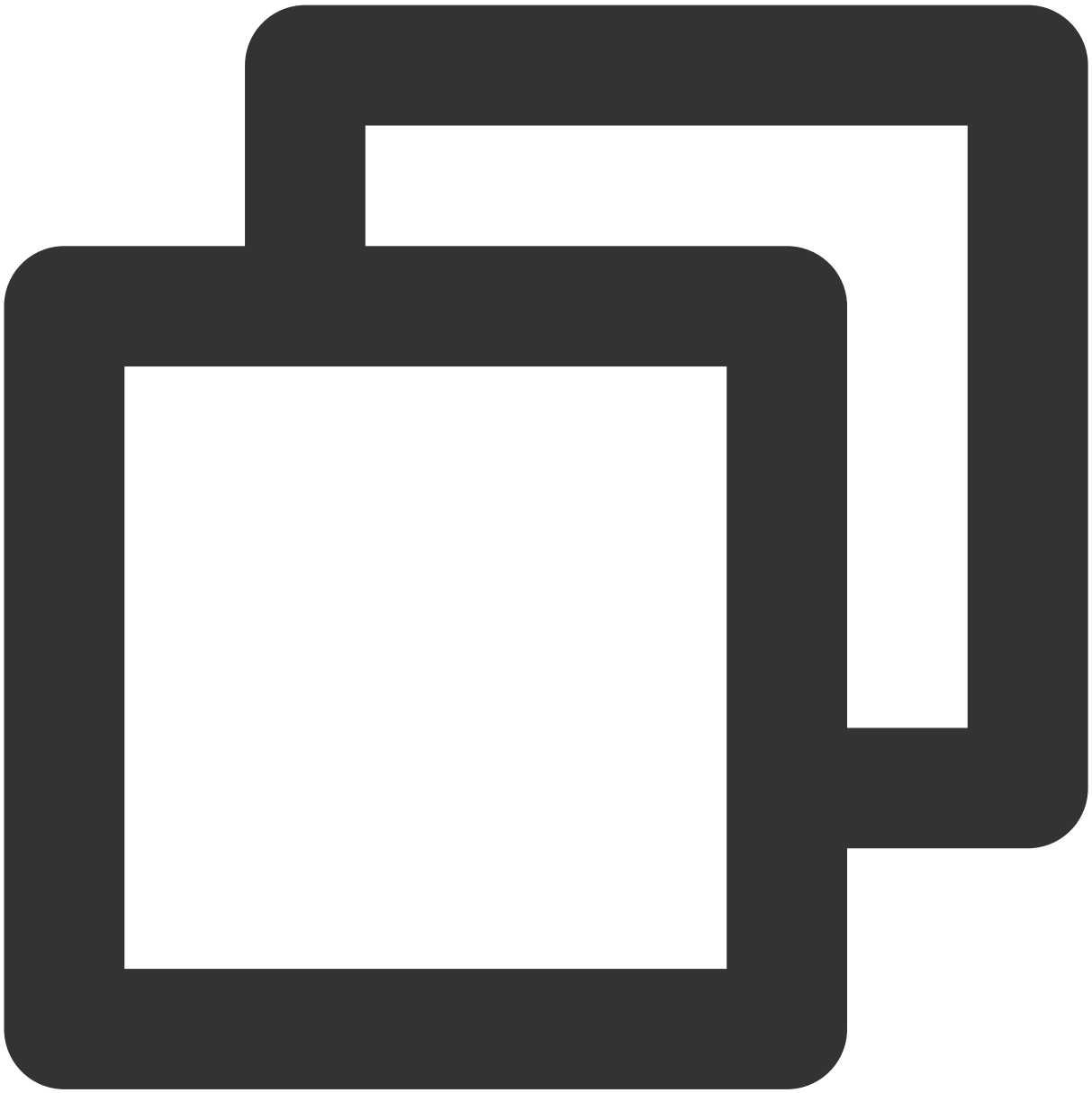
邮箱 OTP 登录场景，发送邮箱验证码用于登录。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic Q0xJRU5UXzRfSUQ6Q0xJRU5UXzRfU0VDUkVU
Host: sample.portal.tencentciam.com

{
"usage" : "login",
"email" : "MOCK_USERNAME@example.com",
"auth_source_id" : "MOCK_EMAIL_OTP_AUTH_SOURCE_ID"
```

```
}
```

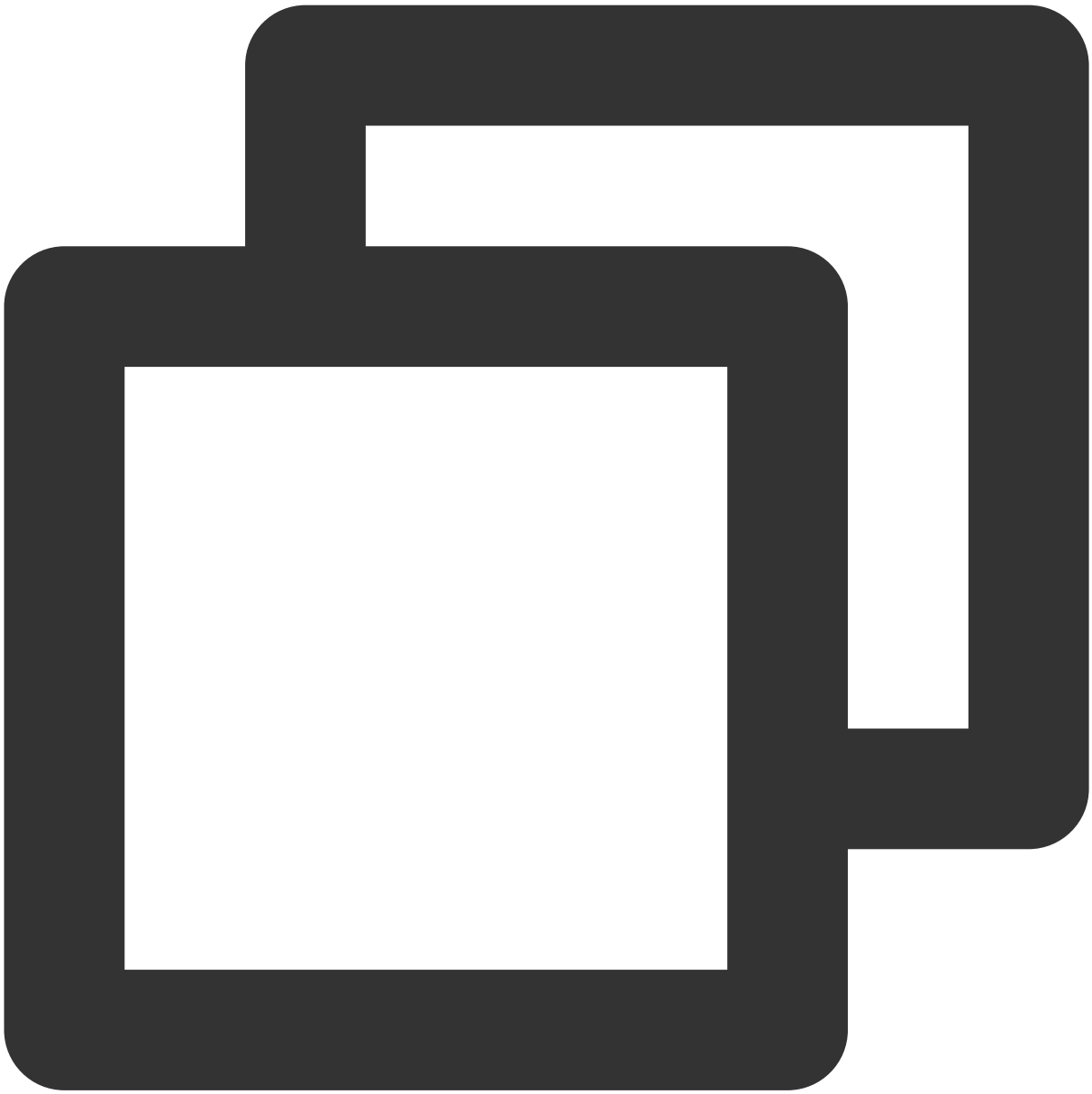
用户注册场景，发送短信验证码用于绑定手机。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic Q0xJRU5UXzRfSUQ6Q0xJRU5UXzRfU0VDUkVU
Host: sample.portal.tencentciam.com

{
"usage" : "signup",
"phone_number" : "13612345678"
```

```
}
```

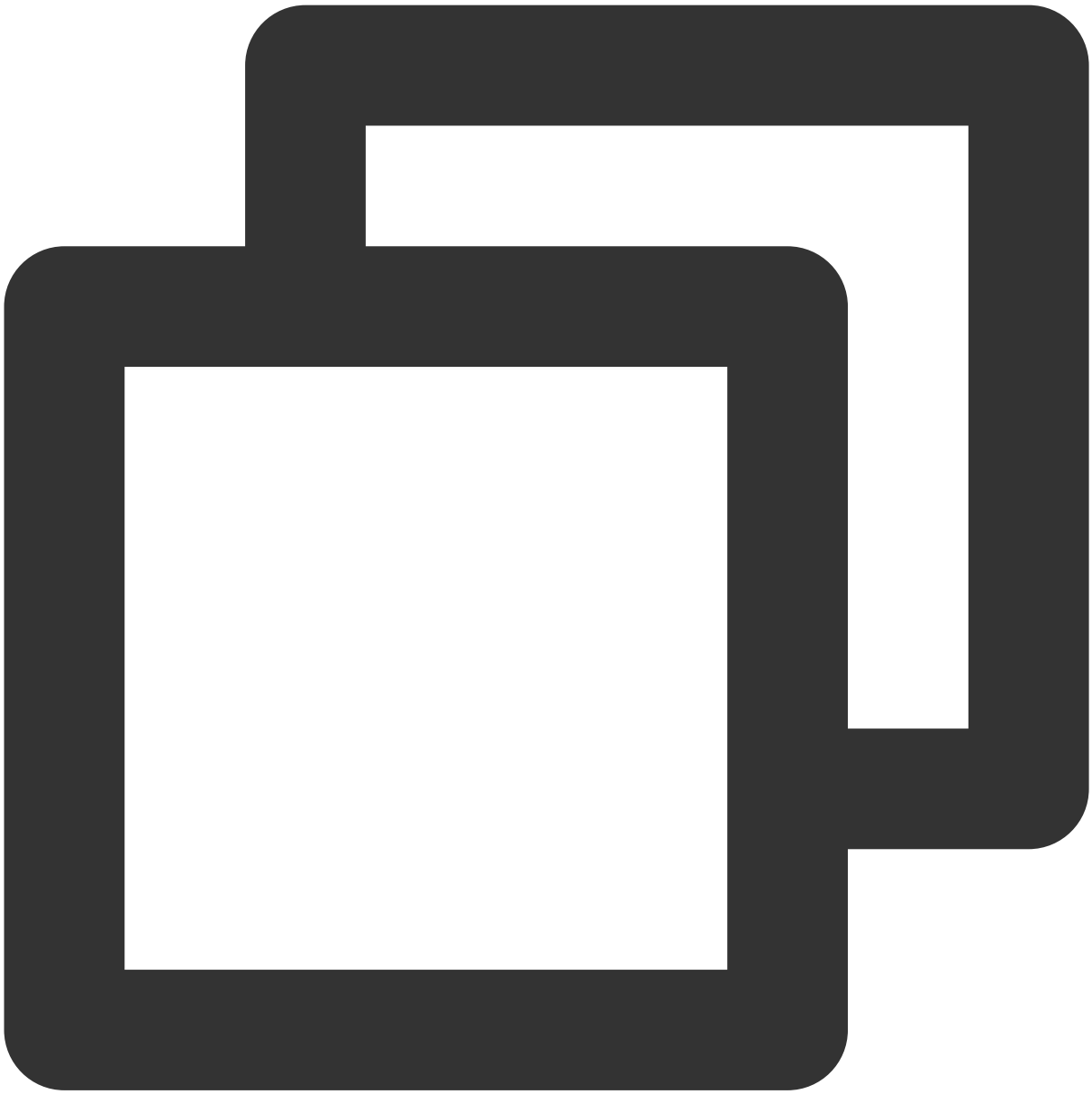
用户注册场景，发送邮箱验证码用于绑定邮箱。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic Q0xJRU5UXzRfSUQ6Q0xJRU5UXzRfU0VDUkVU
Host: sample.portal.tencentciam.com

{
"usage" : "signup",
"email" : "MOCK_USERNAME@example.com"
```

```
}
```

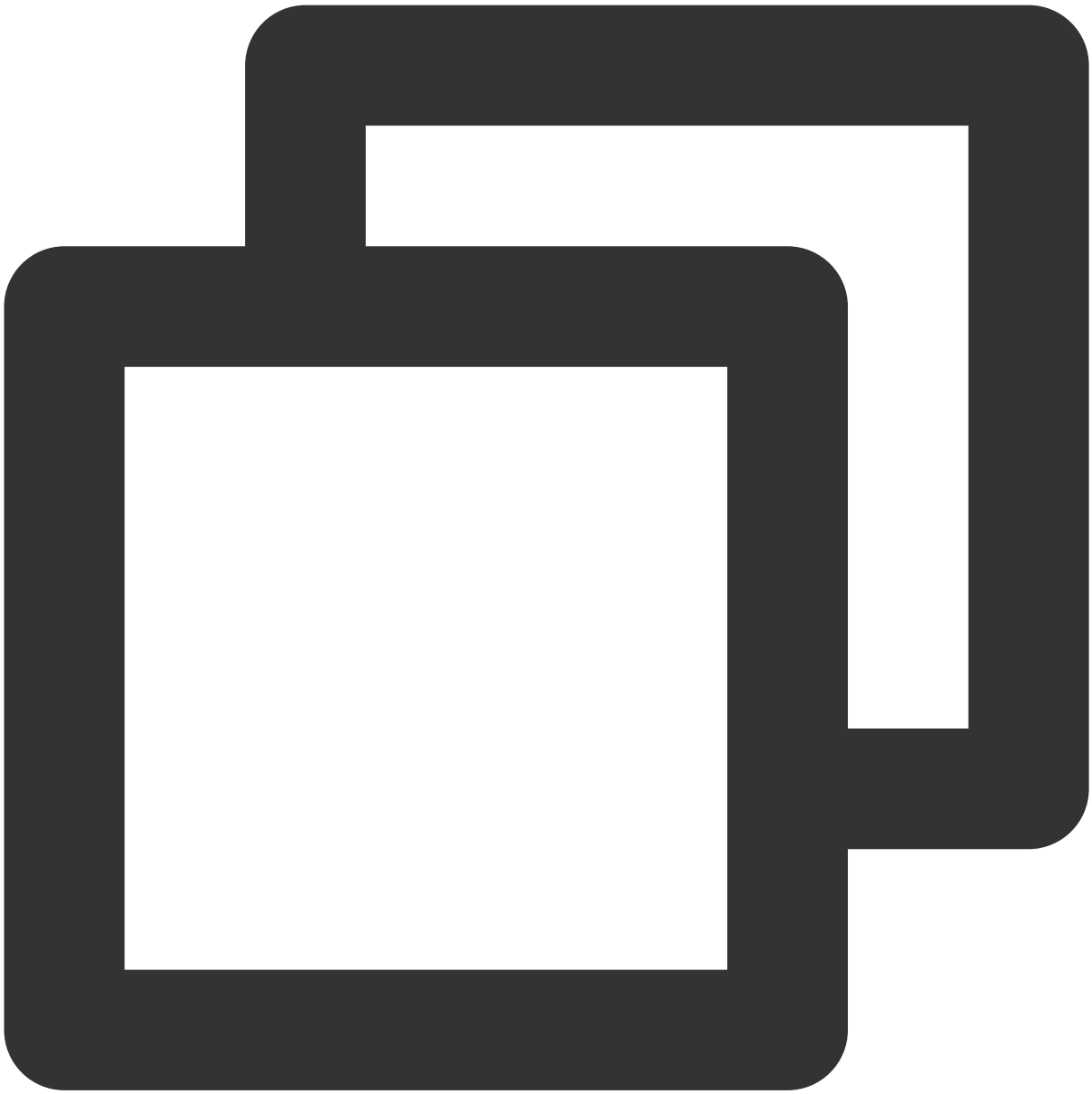
更新用户信息场景，发送短信验证码绑定或更新手机号。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic Q0xJRU5UXzRfSUQ6Q0xJRU5UXzRfU0VDUkVU
Host: sample.portal.tencentciam.com

{
"usage" : "update_userinfo",
"phone_number" : "13612345678"
```

```
}
```

重置密码场景，发送邮箱验证码。



```
POST /otp/send HTTP/1.1
Content-Type: application/json
Authorization: Basic Q0xJRU5UXzRfSUQ6Q0xJRU5UXzRfU0VDUkVU
Host: sample.portal.tencentciam.com

{
"usage" : "reset_password",
"email" : "MOCK_USERNAME@example.com"
```

```
}
```

请求头

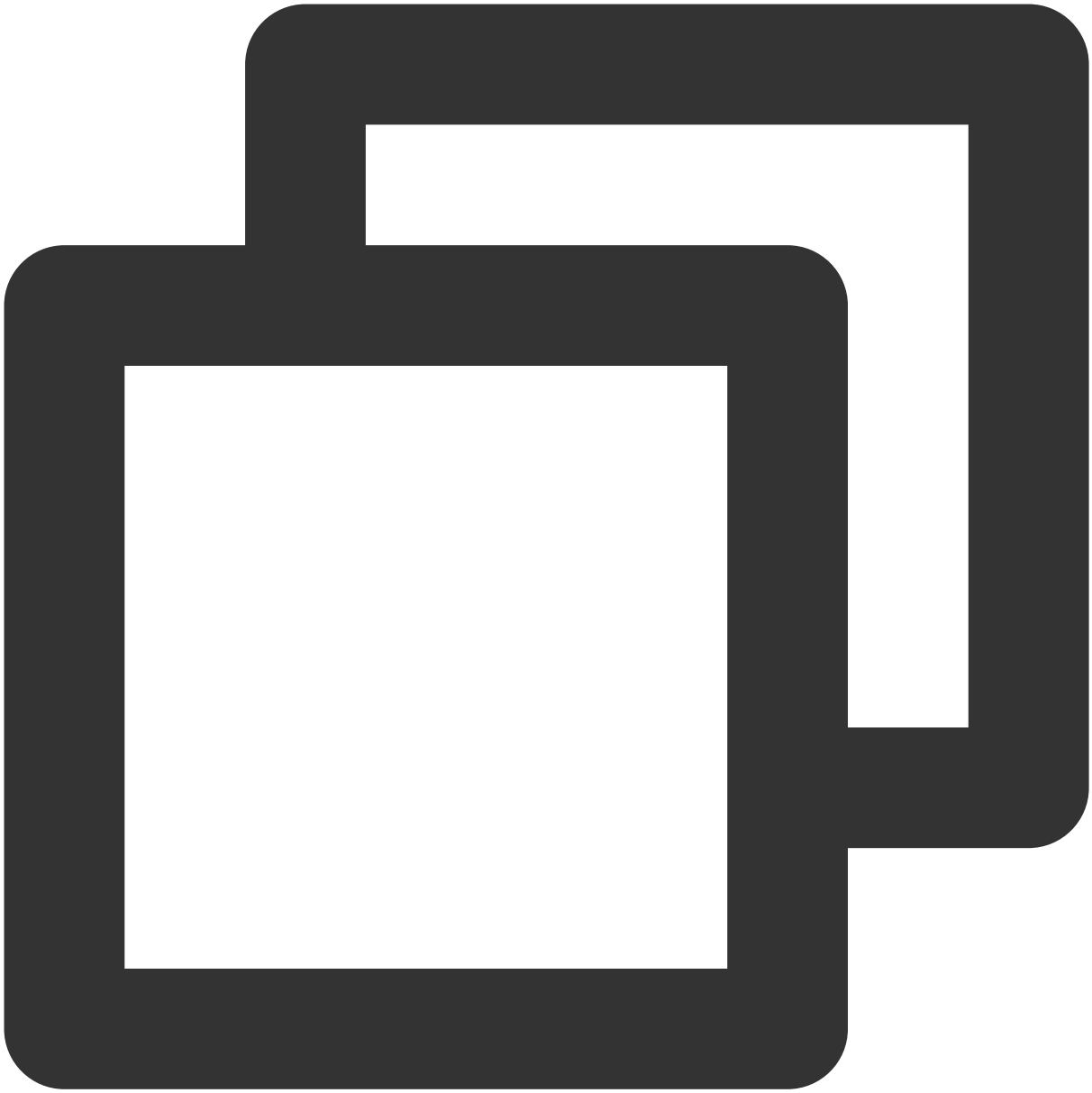
名称	描述
Authorization	HTTP Basic 认证请求头，格式为 `Basic <credentials>` ，其中 `Basic` 为固定字符串， `<credentials>` 的计算方式为 `base64(url_encode(client_id) + ":" + url_encode(client_secret))` ， `Basic` 和 `<credentials>` 之间用一个空格隔开。

请求体 JSON 参数

JSON 路径	数据类型	描述
usage	String	OTP 验证码的使用场景。 短信和邮箱 OTP 登录场景输入 `login` 。 用户注册场景输入 `signup` 。 更新用户信息场景输入 `update_userinfo` 。 重置用户密码场景输入 `reset_password` 。 如果没有输入参数，默认代表登录场景。
phone_number	String	用户的手机号，限国内三大运营商11位手机号。发送短信 OTP 验证码时传递此参数。
email	String	用户的邮箱地址。发送邮箱 OTP 验证码时传递此参数。
auth_source_id	String	短信 OTP 或邮箱 OTP 认证源 ID。可在控制台的通用认证源列表页面查看。 短信和邮箱 OTP 登录场景传递此参数，系统将使用认证源配置的验证码长度和有效期。其他场景不传递此参数，系统默认使用6位数字验证码，有效期60秒。

正常响应示例

验证码发送成功。



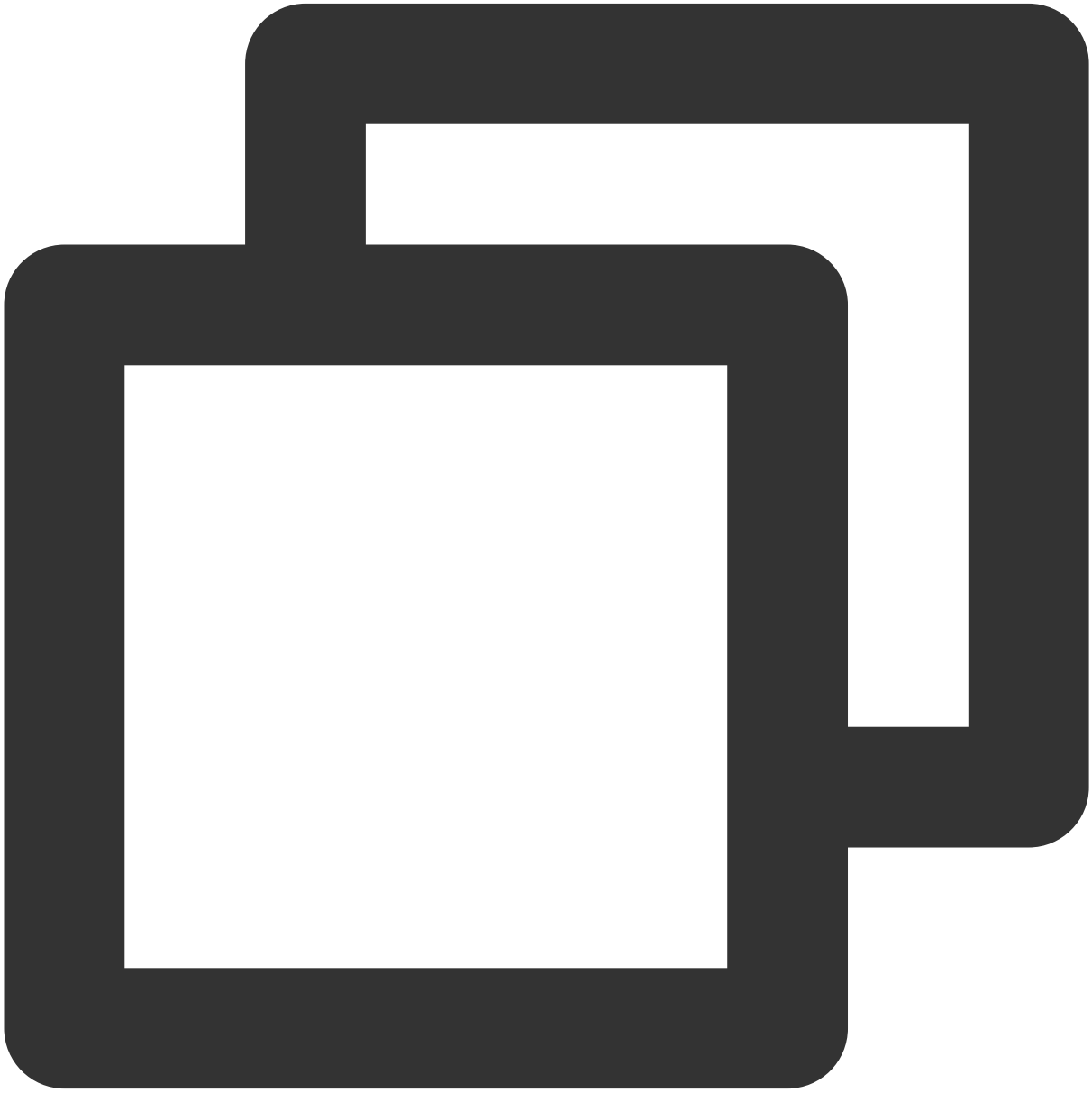
```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "otp_token" : "MOCK_OTP_TOKEN"
}
```

响应参数

字段	数据类型	描述
otp_token	String	OTP token，后续验证 OTP 时携带使用。有效期5分钟。

异常响应示例

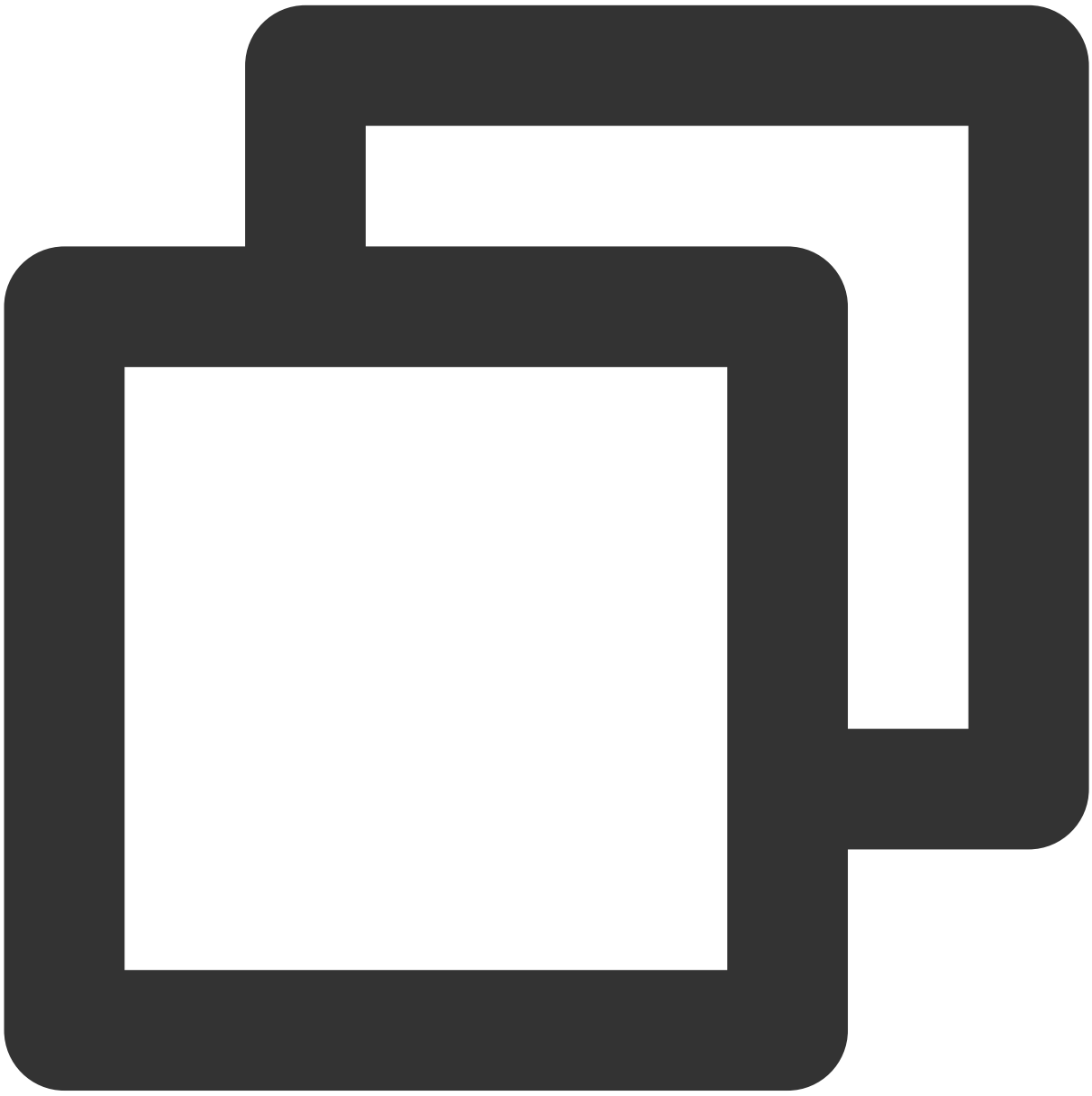
手机号格式有误。



```
HTTP/1.1 400 Bad Request
```

```
Content-Type: application/json;charset=UTF-8

{
"error" : "malformed_phone_number"
}
```

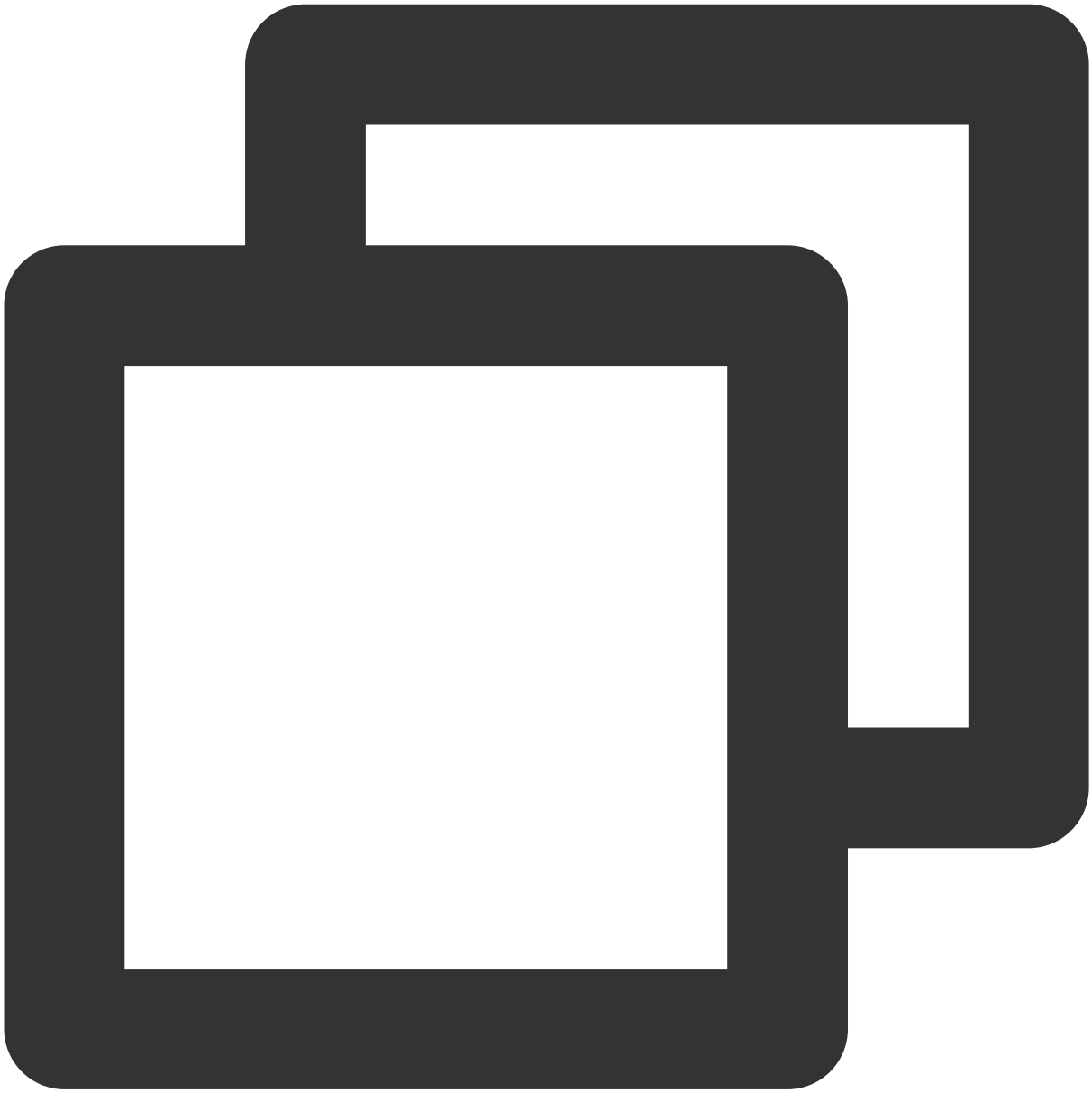
邮箱格式有误。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
```

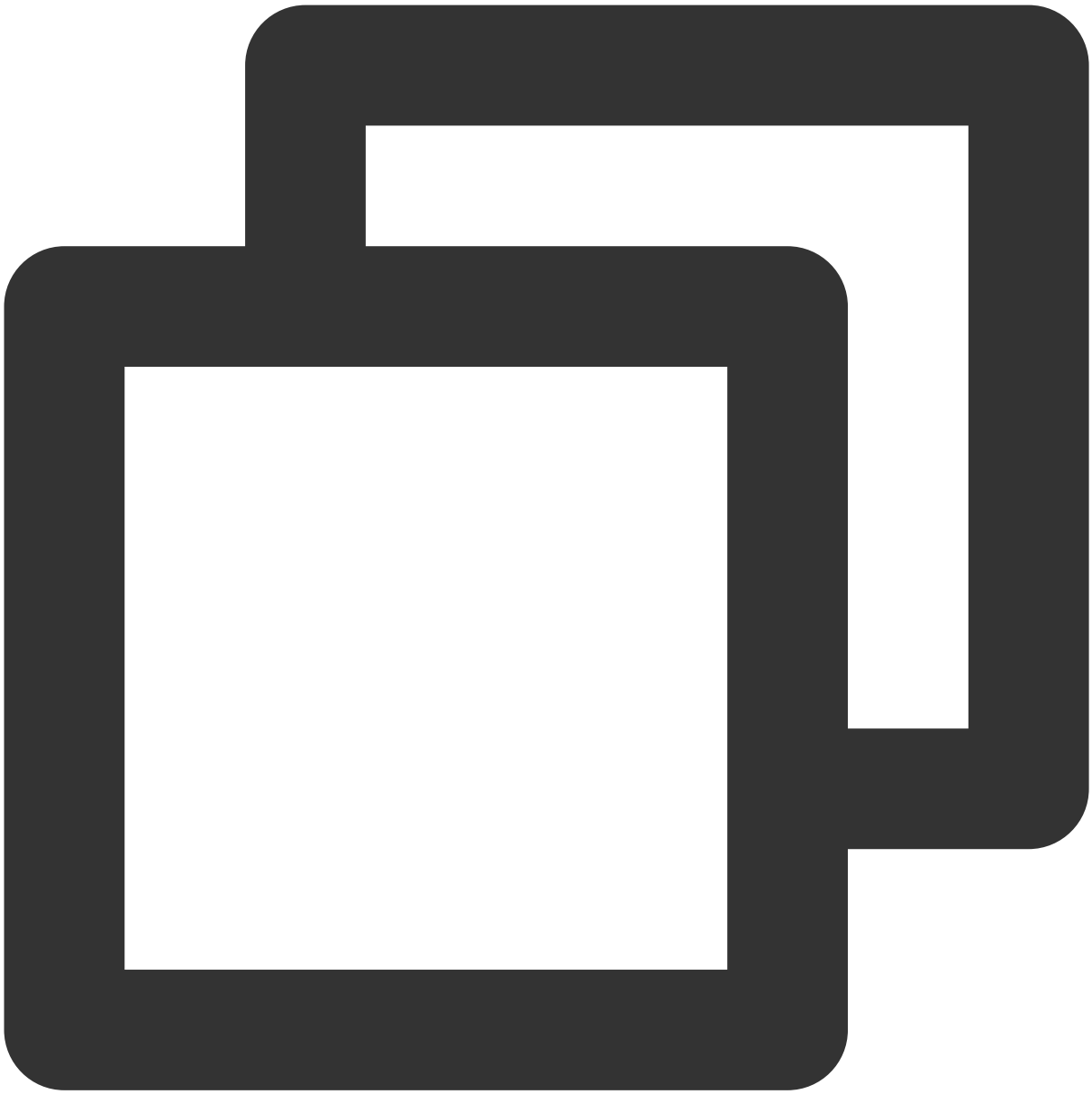
```
"error" : "malformed_email"
}
```

因短信额度不足无法发送短信，一般是由于免费短信额度已用尽，需要到控制台配置 短信模板。



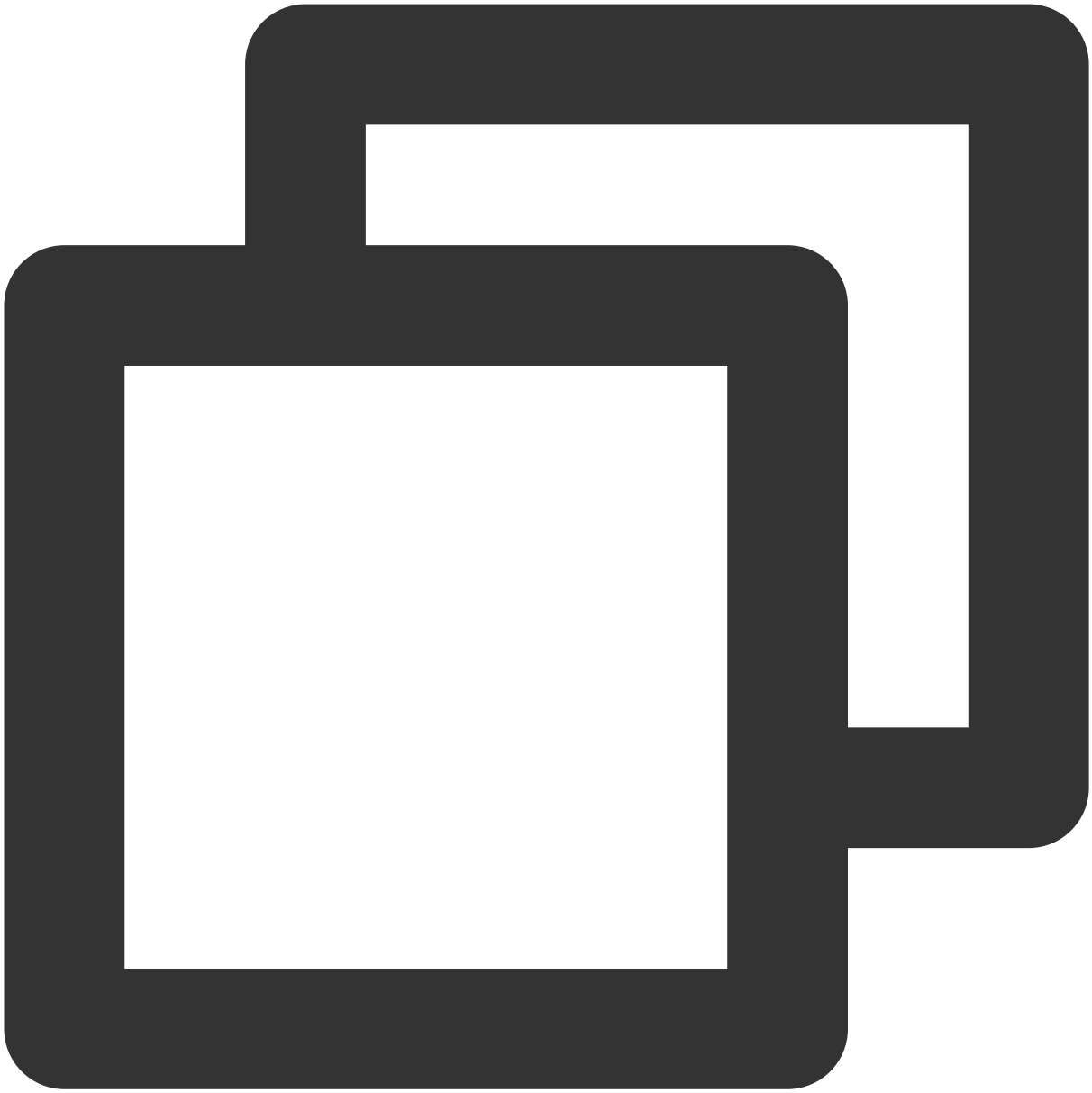
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "insufficient_sms_quota"
}
```

因邮箱额度不足无法发送邮件，一般是由于免费邮箱额度已用尽，需要到控制台配置 邮箱模板。



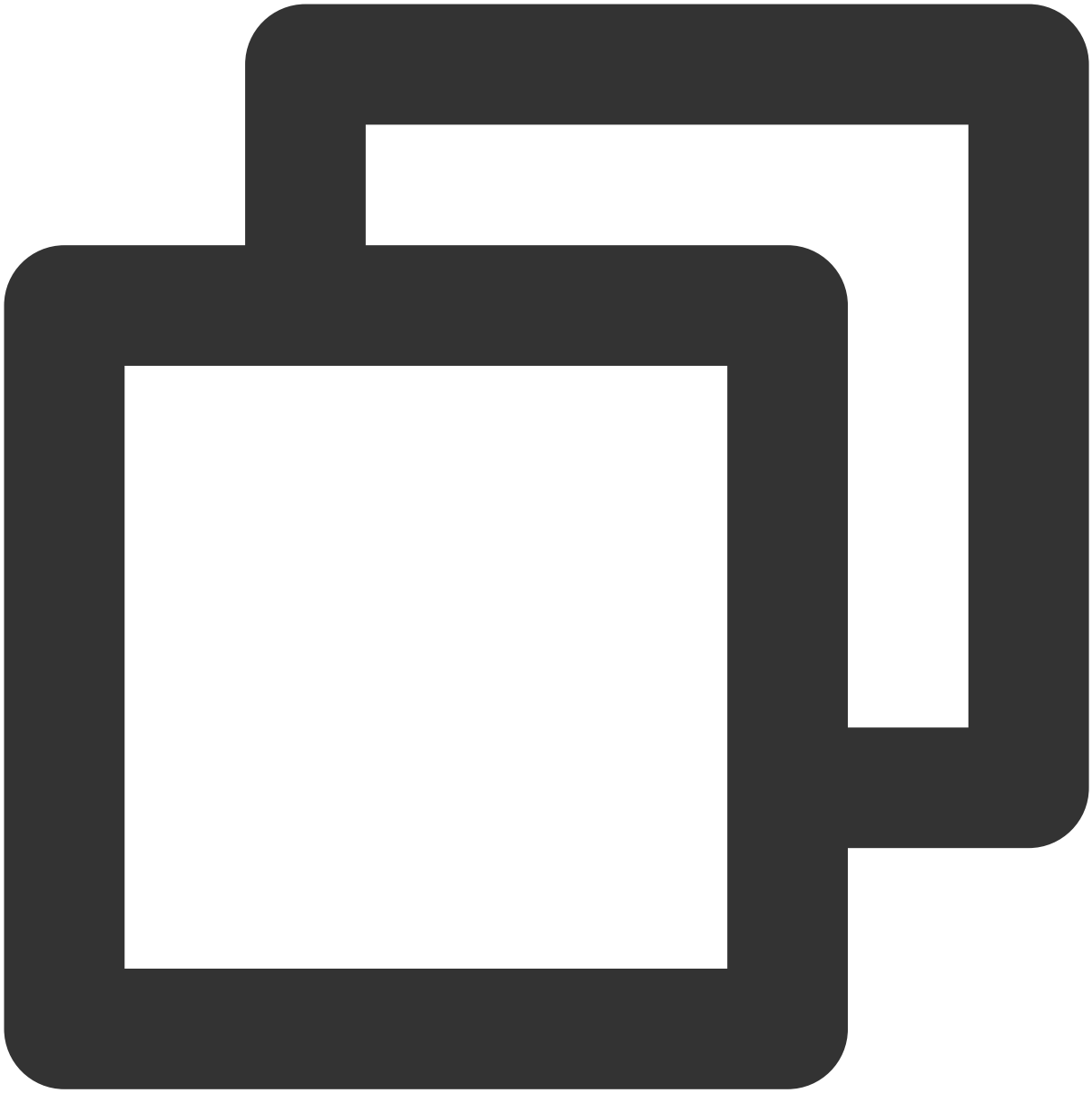
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "insufficient_email_quota"
}
```

邮箱地址不存在或在黑名单中。



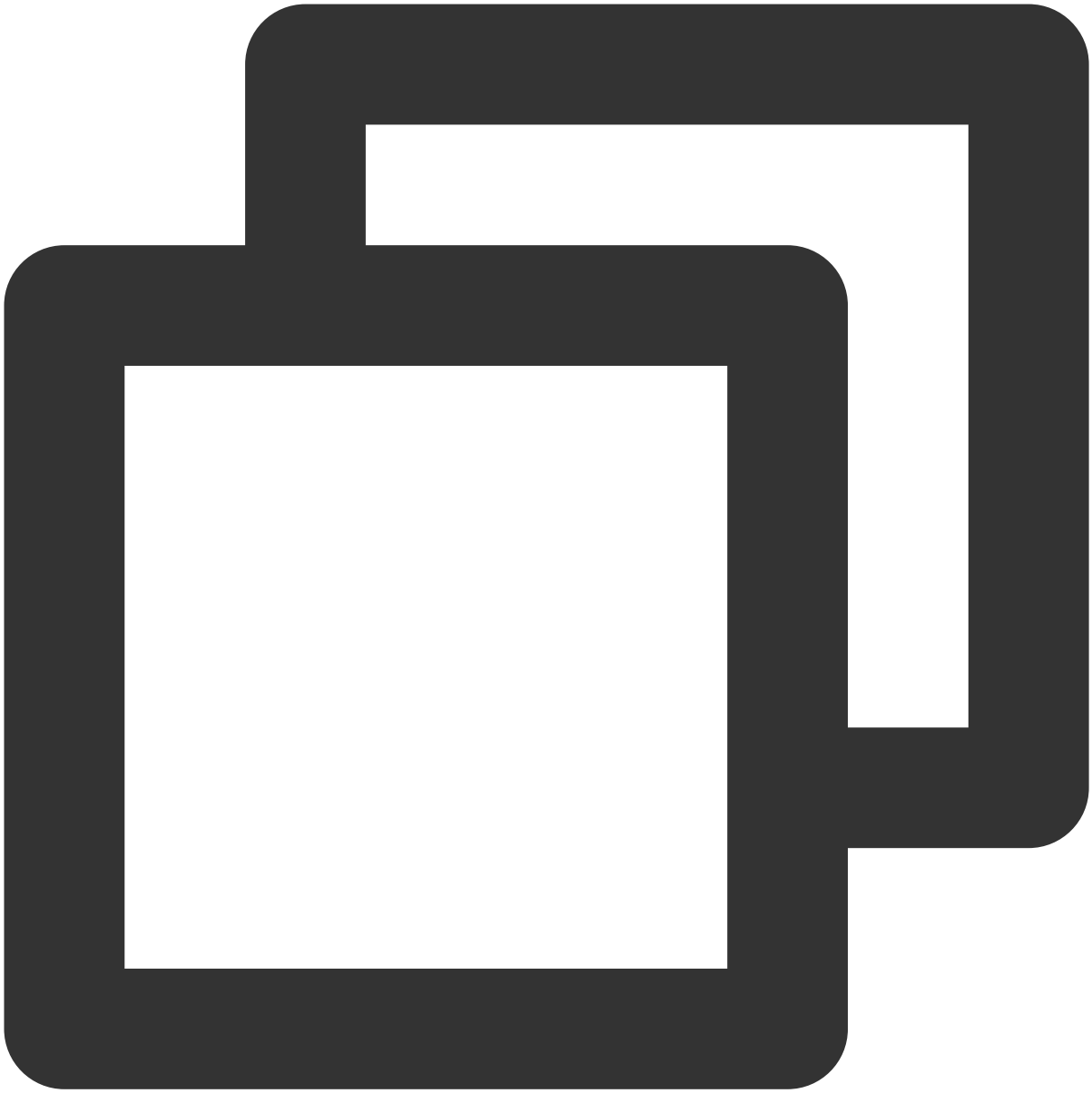
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_email"
}
```

验证码发送失败。



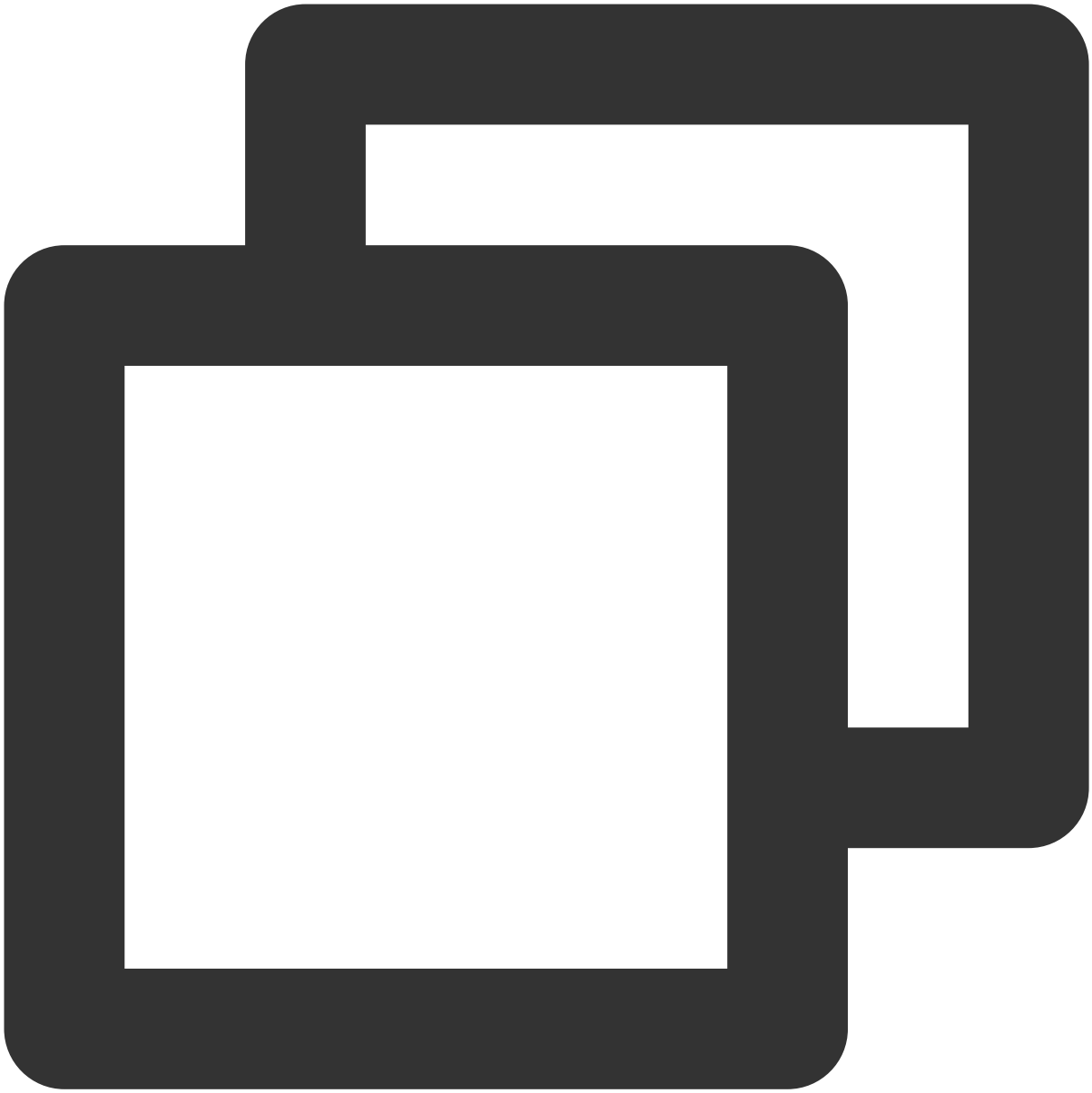
```
HTTP/1.1 503 Service Unavailable
Content-Type: application/json;charset=UTF-8

{
"error" : "temporarily_unavailable",
"error_description" : "Failed to send OTP. Please try again later."
}
```

注册场景，邮箱被使用。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
  "error": "email_is_used"
}
```

注册场景，手机号被使用。

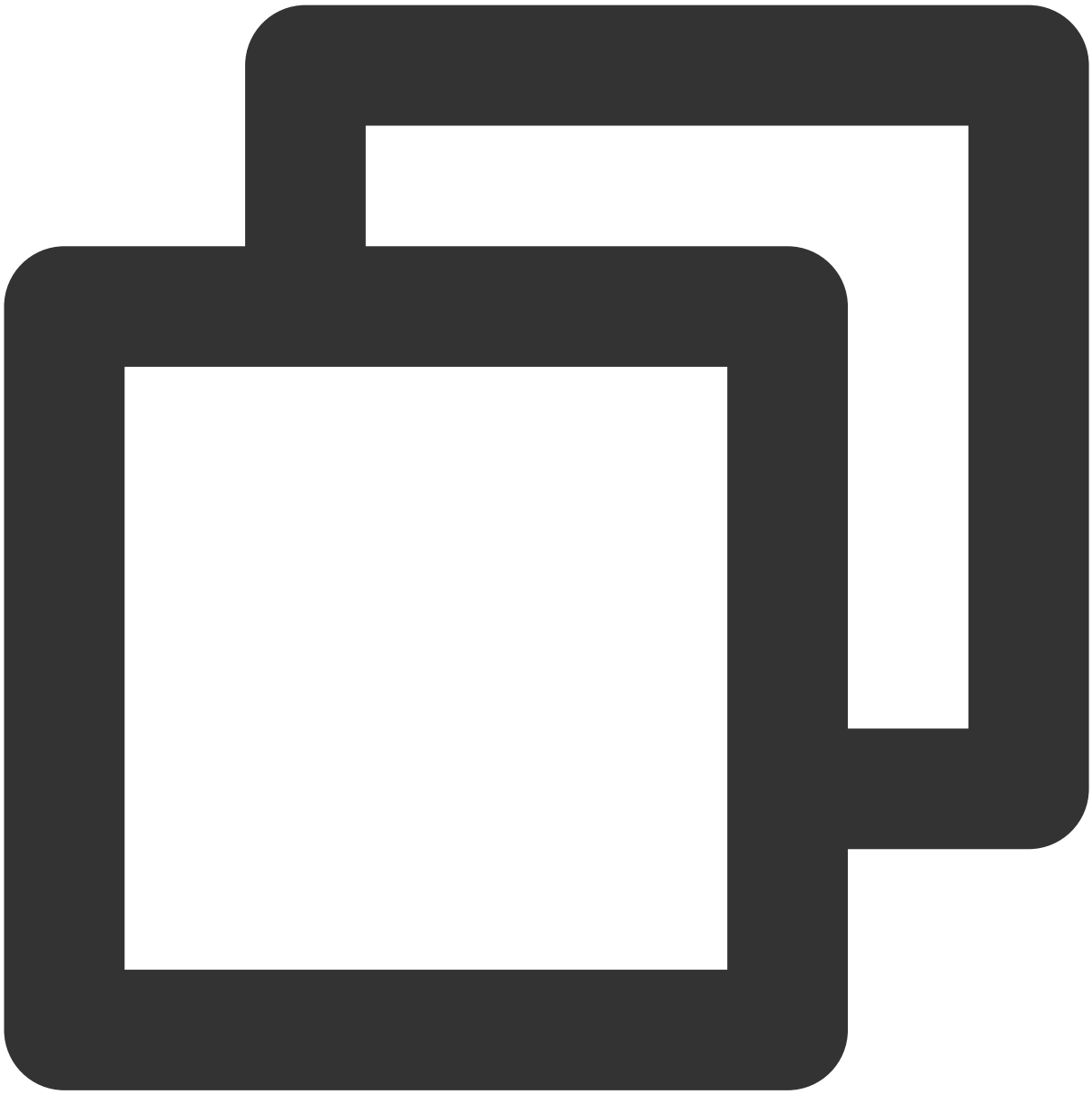


```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8


{
  "error": "phone_number_is_used"
}
```

向单个手机号发送短信频率超限。

如果使用的是自购短信服务，可自行到 短信控制台 调整短信频率限制策略。

如果使用的是免费短信额度，频率限制为：对同一手机号，每个自然日内发送短信条数不超过50条；相同内容短信对同一手机号，30秒内发送短信条数不超过1条。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "sms_rate_limit_exceeded",
"error_description" : "SMS rate limit exceeded for same phone number"
}
```

获取用户信息

最近更新时间：2023-12-22 11:42:08

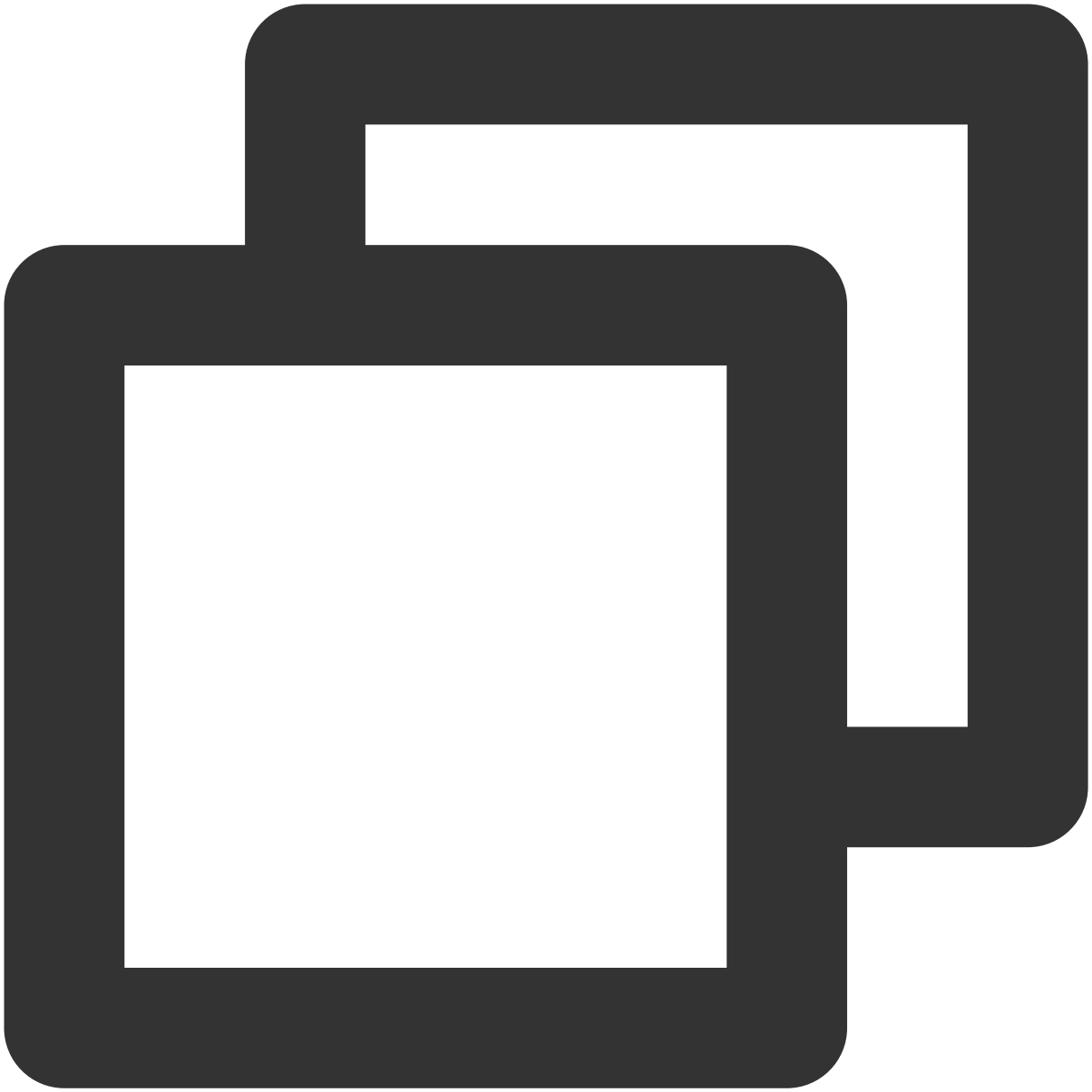
接口描述

获取已登录用户的用户信息。调用此接口时，需携带登录成功时得到的具备 `openid scope` 的 Access Token。

支持的应用类型

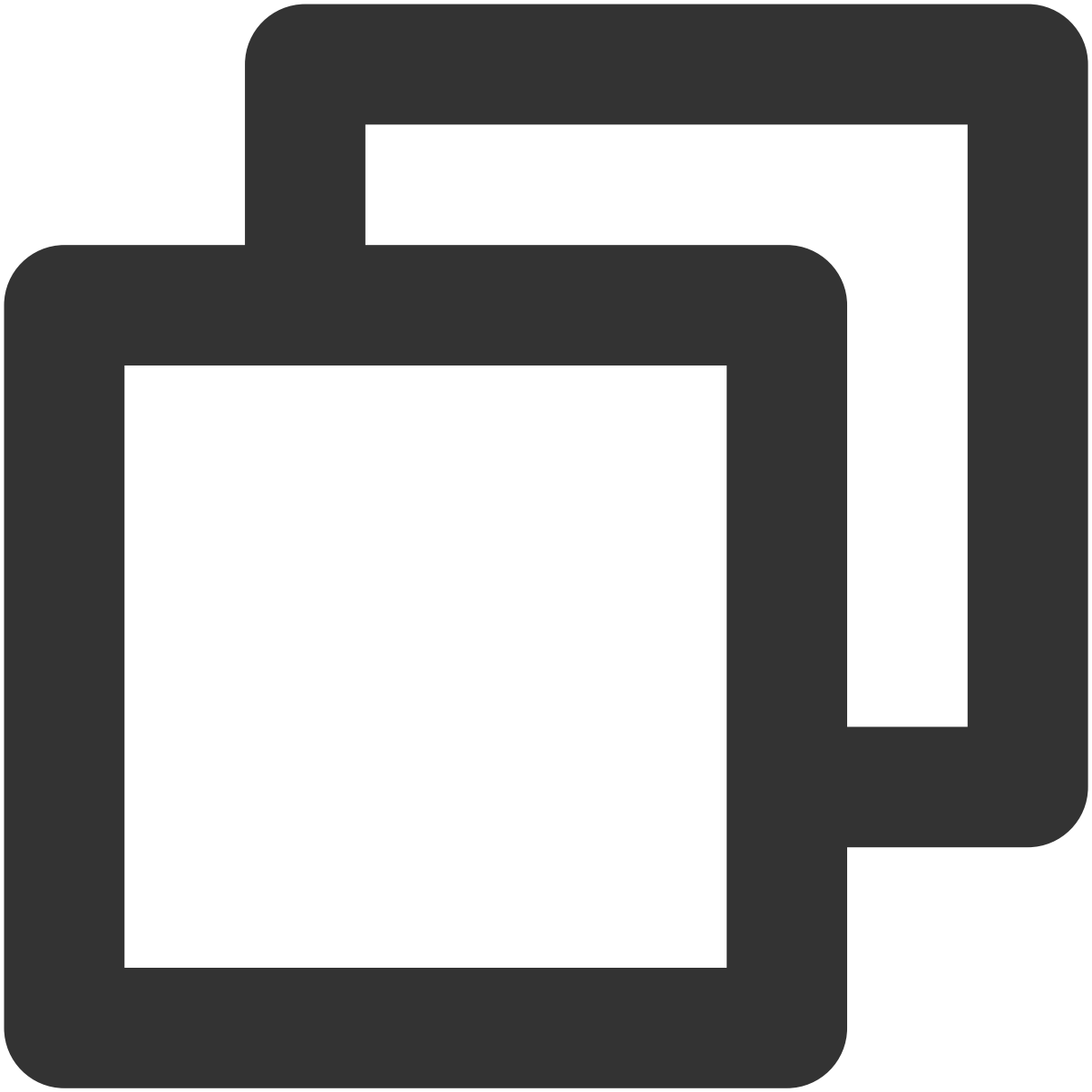
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



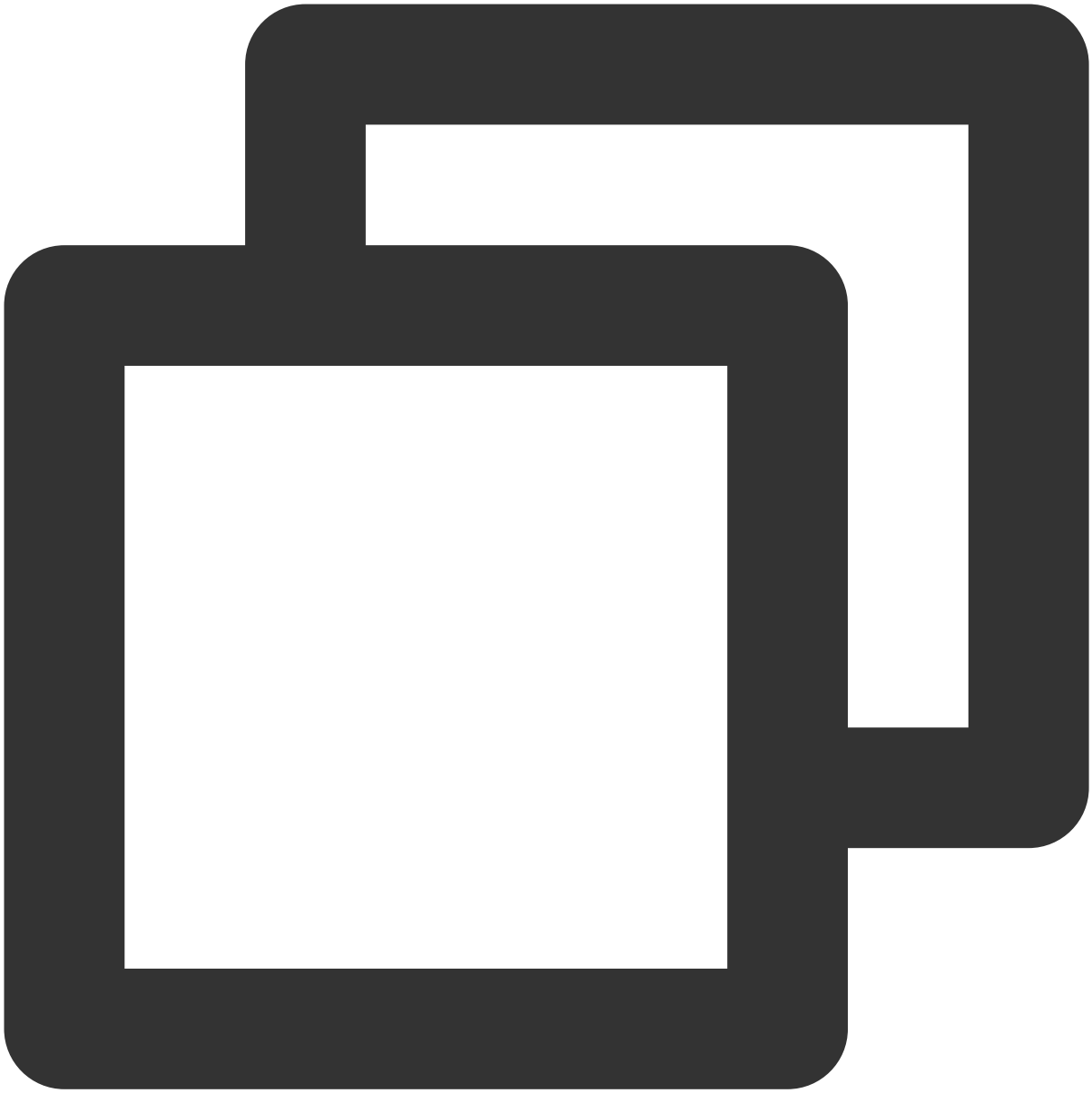
```
GET
```

请求路径



```
/userinfo
```

请求示例



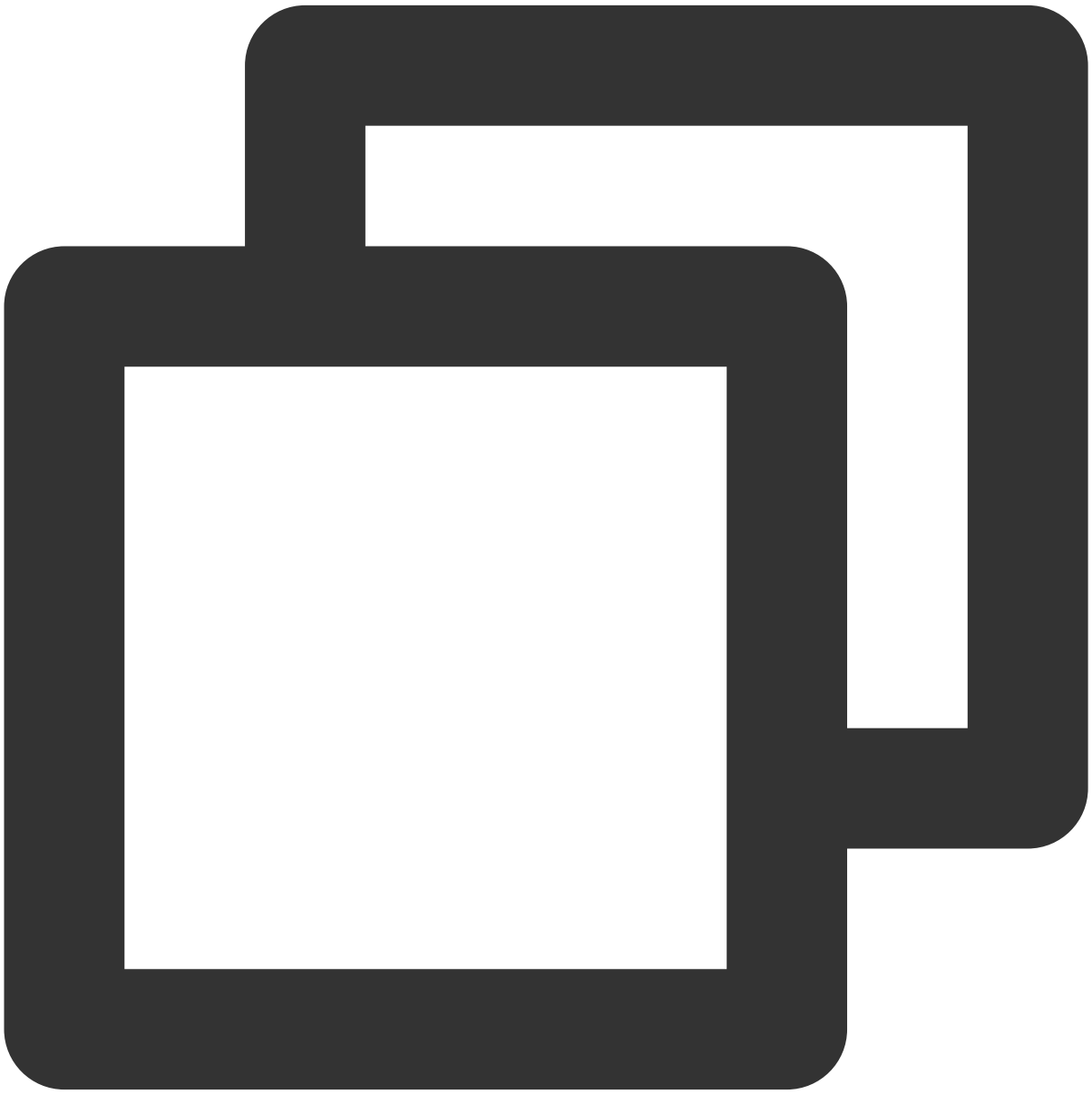
```
GET /userinfo HTTP/1.1
Authorization: Bearer ACCESS_TOKEN_WITH_OPENID_SCOPE
Host: sample.portal.tencentciam.com
```

请求头

名称	描述

Authorization	OAuth 2.0 Bearer Token，格式为 `Bearer <Token>`，其中 `Bearer` 为固定字符串，`<Token>` 为用户登录成功时得到的具备 `openid scope` 的 Access Token，`Bearer` 和 `<Token>` 之间用一个空格隔开。

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json
```

```
{
  "sub" : "MOCK_USER_ID",
  "email" : "MOCK_USERNAME@example.com",
  "name" : "MOCK_NAME",
  "nickname" : "MOCK_NICKNAME",
  "zoneinfo" : "Asia/Shanghai",
  "locale" : "zh-CN"
}
```

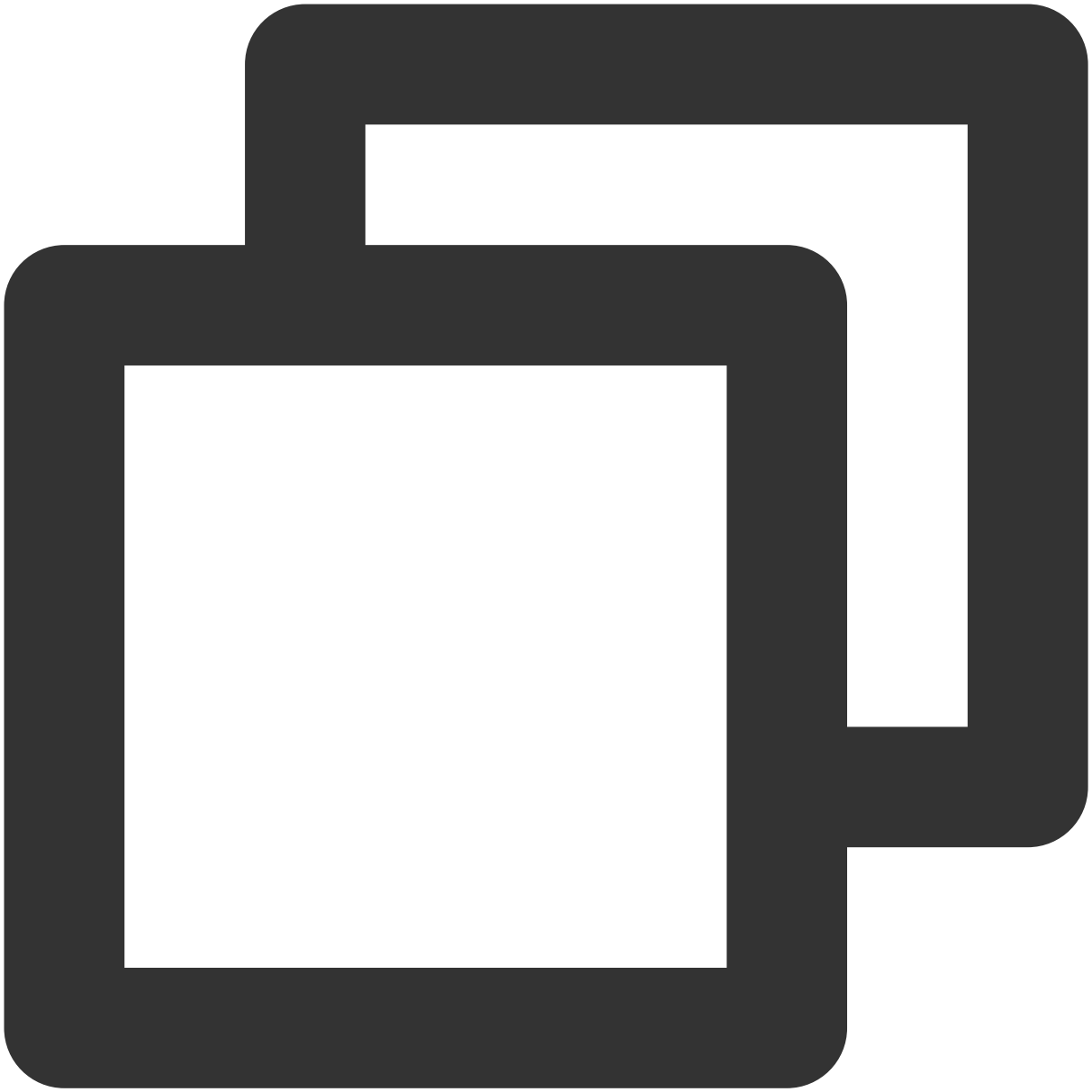
响应参数

参数	数据类型	描述
sub	String	用户标识，在用户池内唯一。

说明：
除 `sub` 字段一定返回外，其余返回哪些字段由应用参数配置中的 `Claims` 决定。

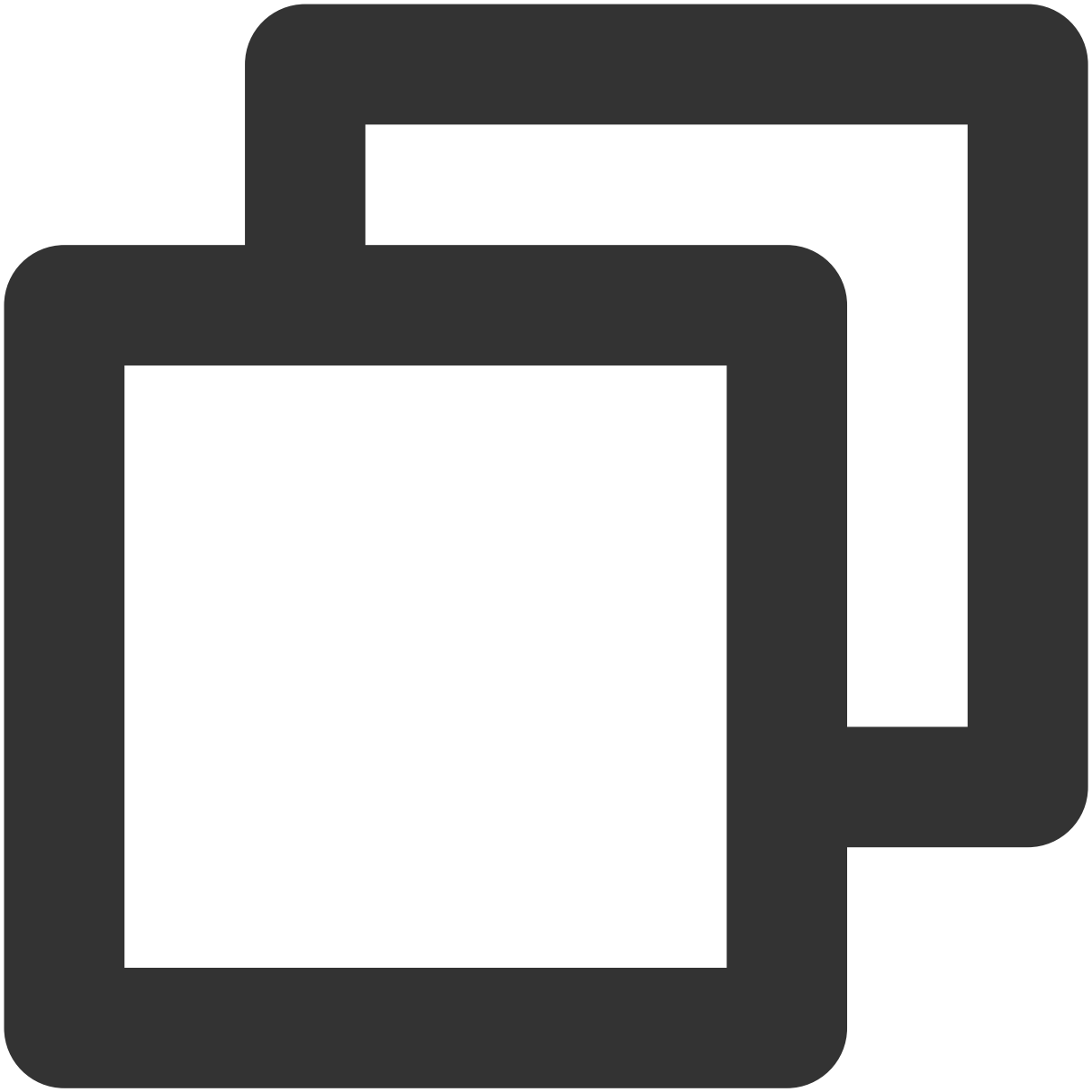
异常响应示例

未携带 Access Token。



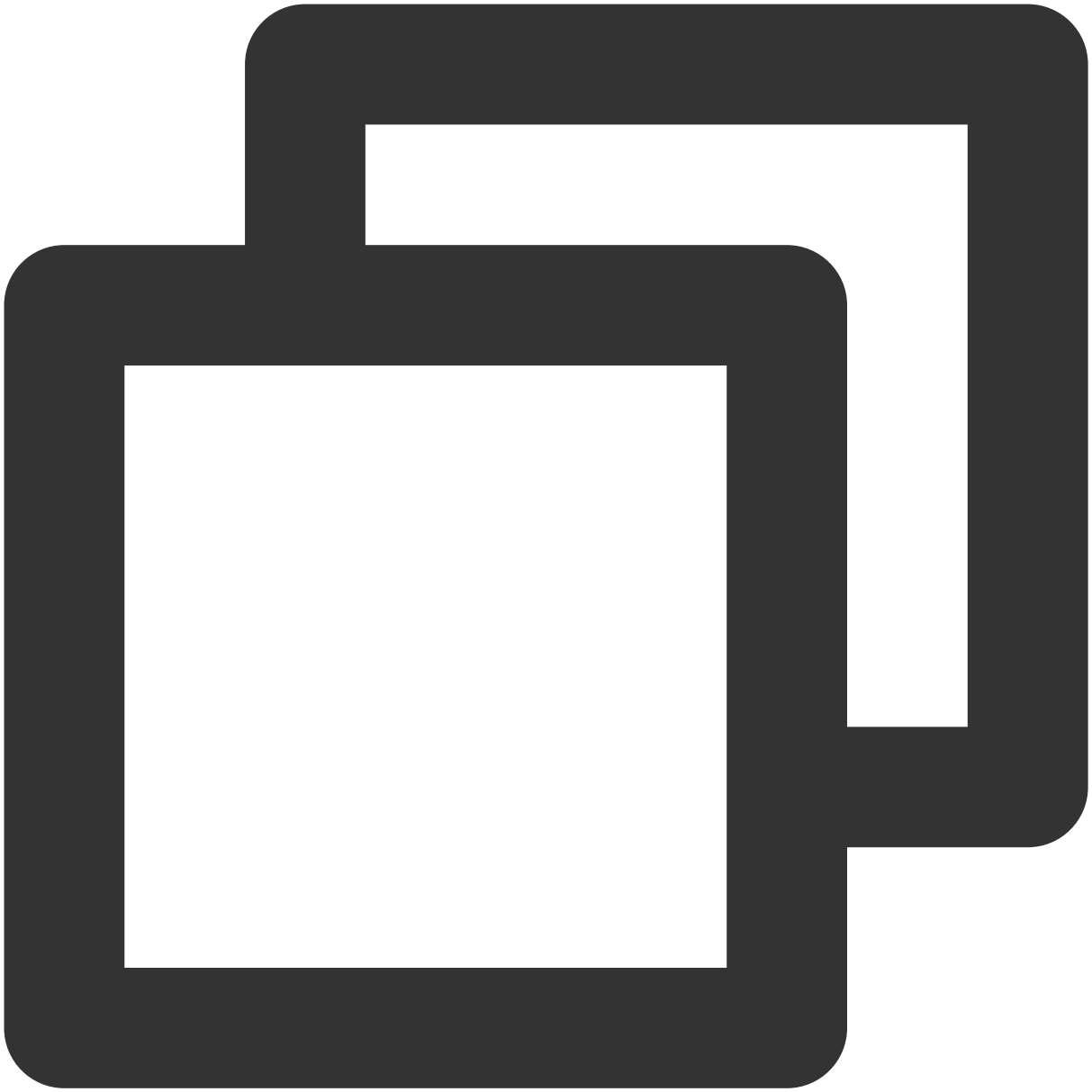
```
HTTP/1.1 400 Bad Request
WWW-Authenticate: Bearer error="invalid_request", error_description="Bearer token n
```

Access Token 无效（例如 Token 格式有误、已过期或已注销）。



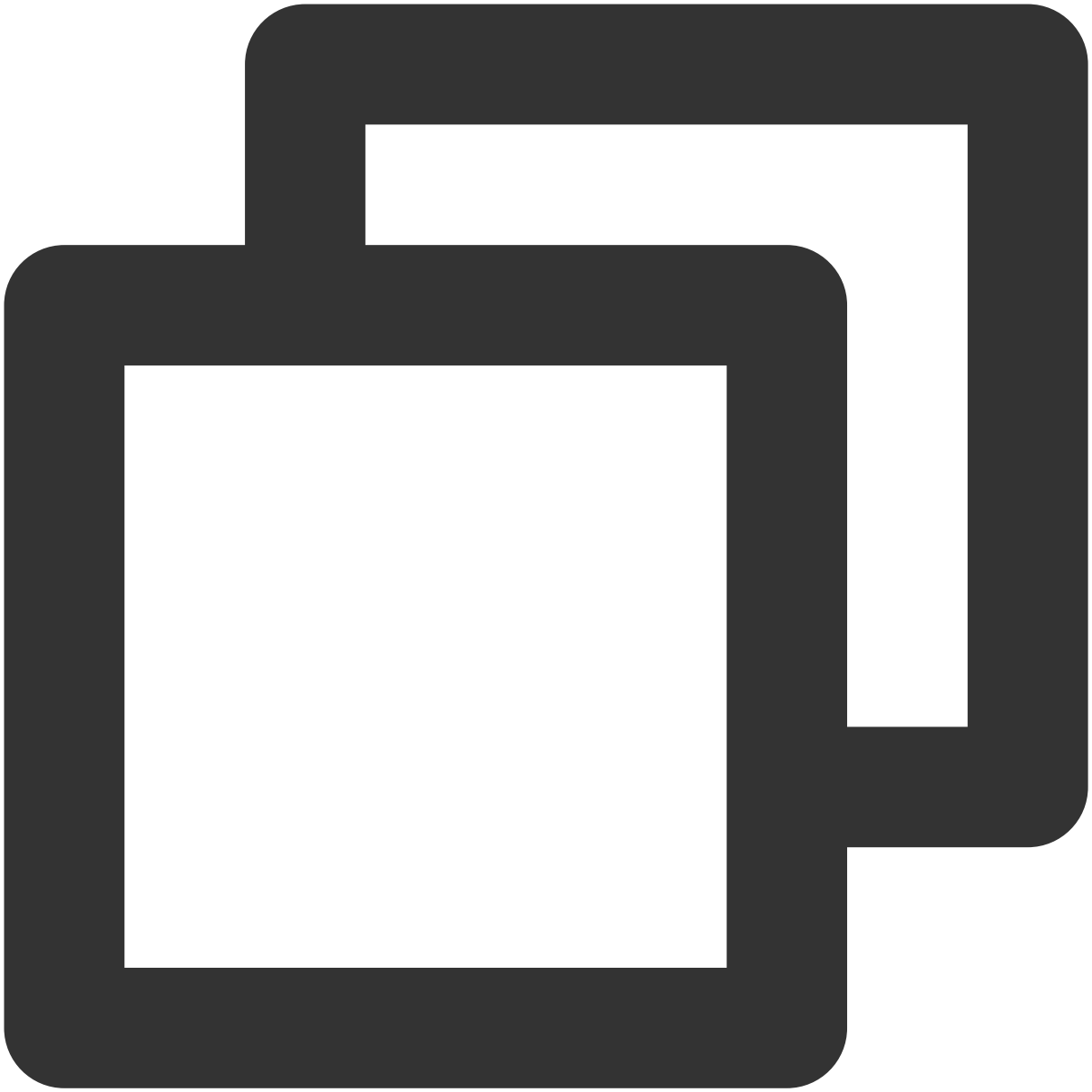
```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="invalid_token", error_description="Error decoding J
```

Access Token 不具备 `openid scope` 。



```
HTTP/1.1 403 Forbidden
WWW-Authenticate: Bearer error="insufficient_scope", error_description="The request
```

找不到 Access Token 对应的用户。



```
HTTP/1.1 404 Not Found
Content-Type: application/json;charset=UTF-8

{
"error" : "user_not_found"
}
```

更新用户信息

最近更新时间：2023-12-22 11:42:07

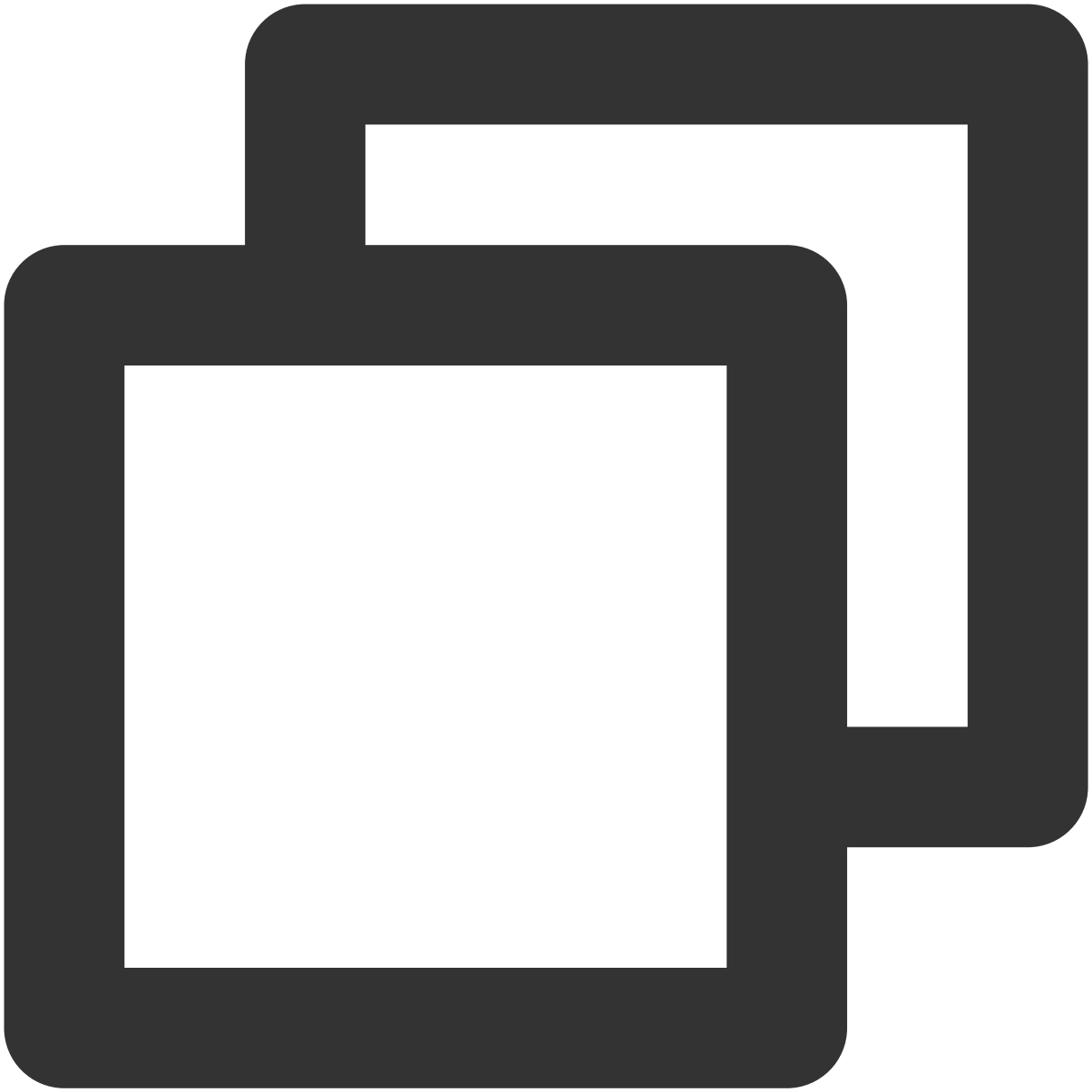
接口描述

更新已登录用户的个人信息。调用此接口时，需携带登录成功时得到的具备 openid scope 的 Access Token。如果更新手机号或邮箱，则需先调用 发送 OTP 验证码 接口向用户发送验证码。

支持的应用类型

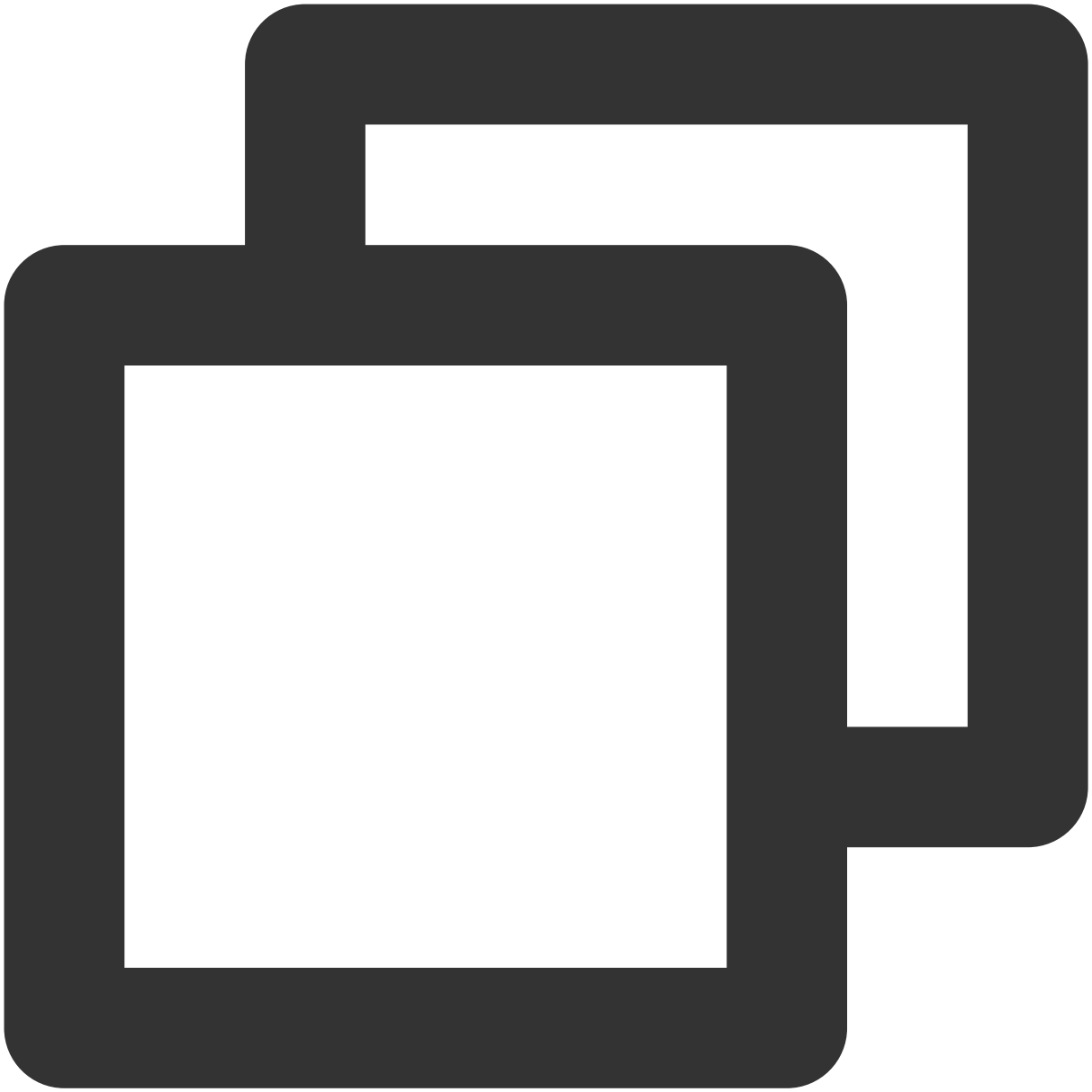
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



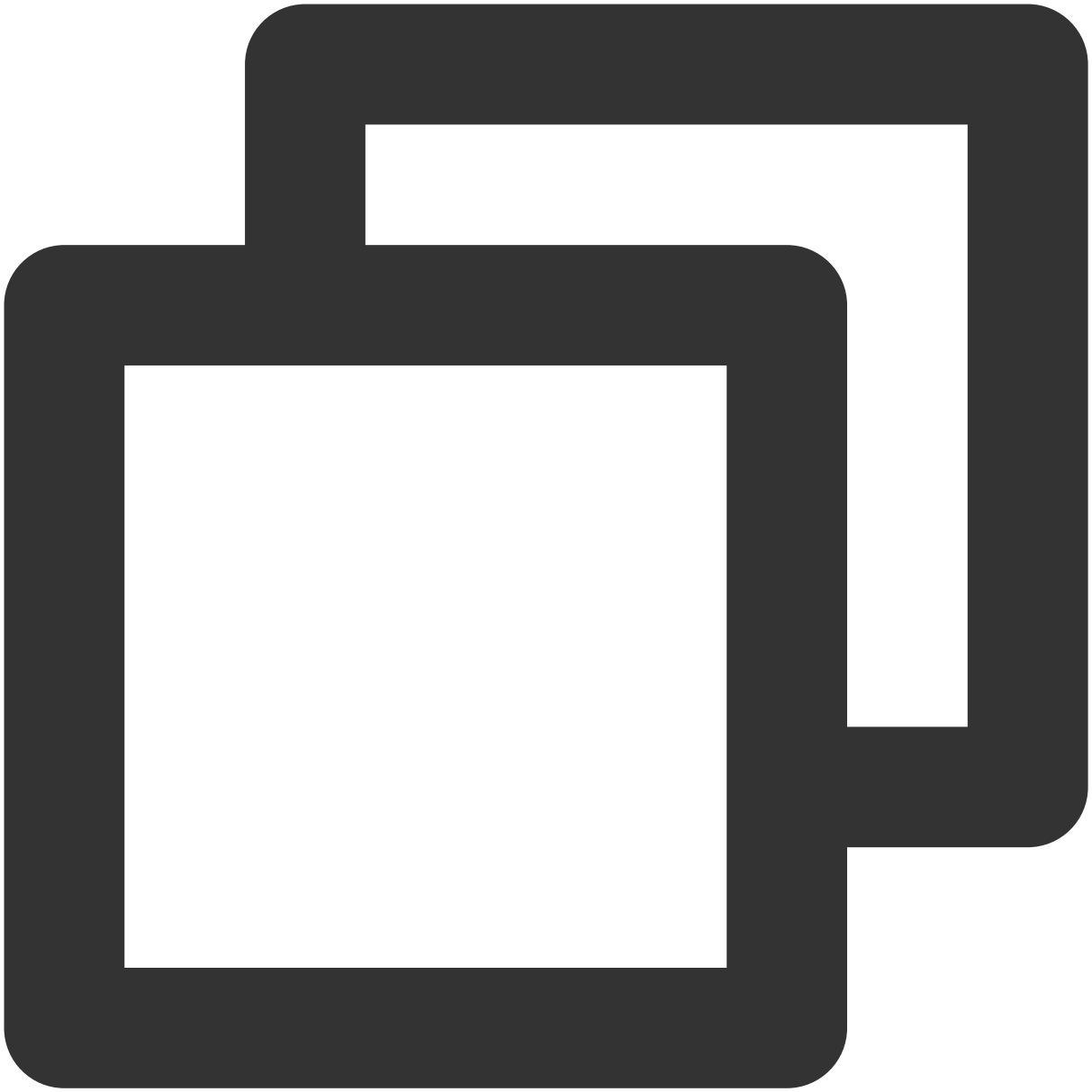
```
PATCH
```

请求路径



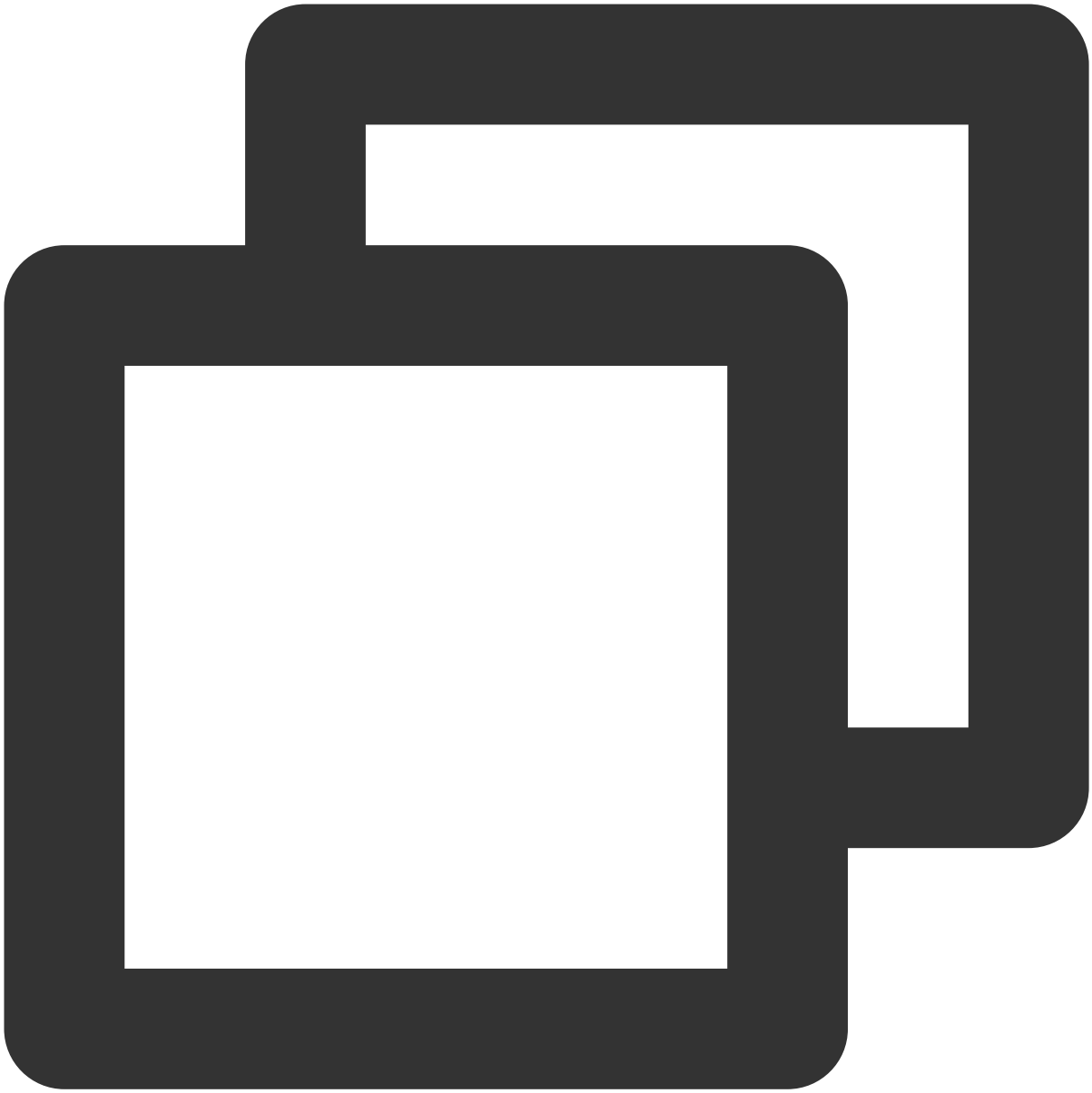
```
/userinfo
```

请求 Content-Type



```
application/json
```

请求示例



```
PATCH /userinfo HTTP/1.1
Content-Type: application/json
Authorization: Bearer ACCESS_TOKEN_WITH_OPENID_SCOPE
Host: sample.portal.tencentciam.com

{
  "nickname" : "MOCK_NICKNAME"
}
```

请求头

名称	描述
Authorization	OAuth 2.0 Bearer Token，格式为 `Bearer <Token>`，其中 `Bearer` 为固定字符串，`<Token>` 为用户登录成功时得到的具备 `openid scope` 的 `Access Token`，`Bearer` 和 `<Token>` 之间用一个空格隔开。

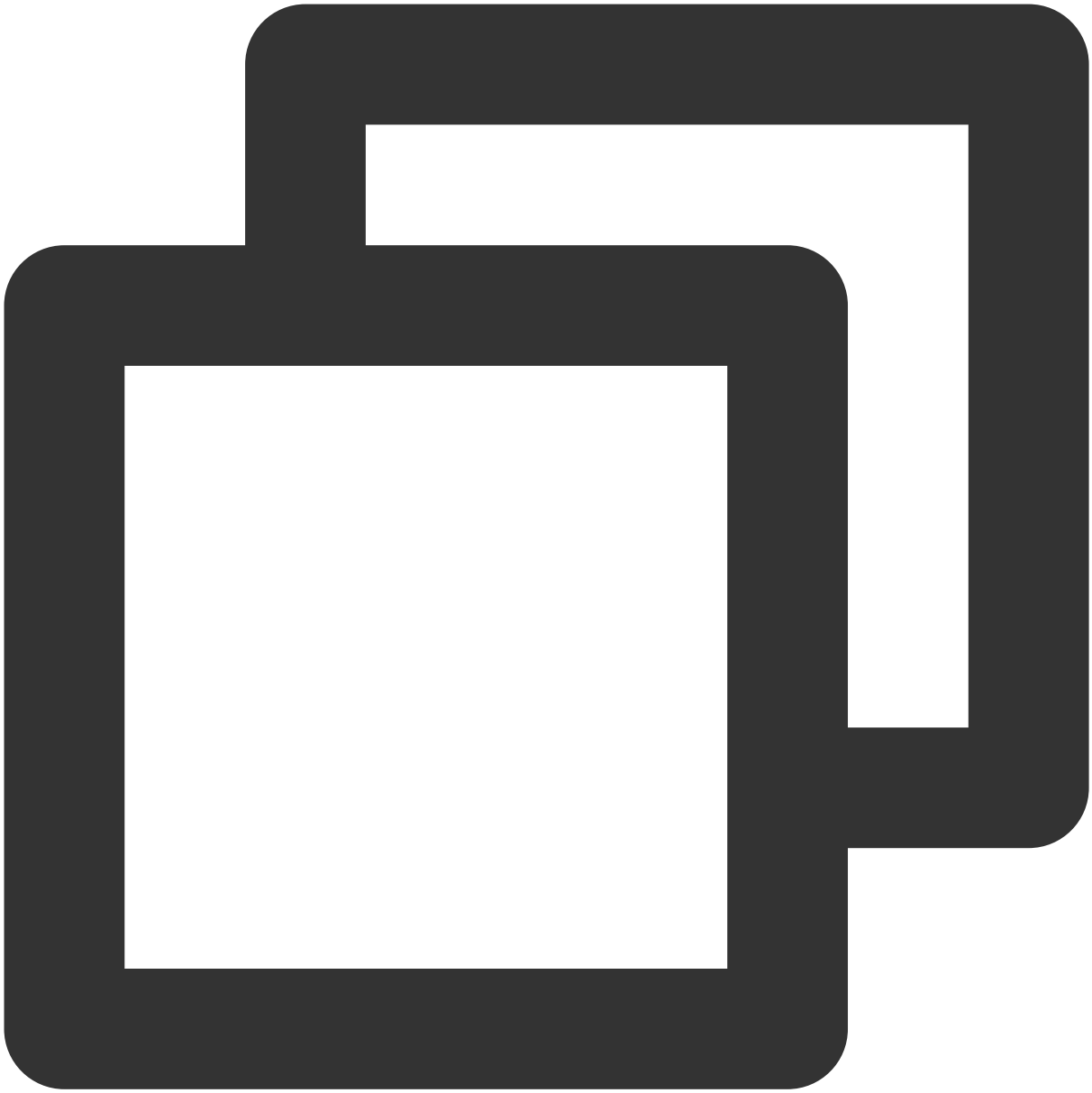
请求体 JSON 参数

JSON 路径	数据类型	描述
phone_number	String	用户的手机号，限国内三大运营商11位手机号。传递此参数时，须同时传递 `phone_number_otp_token` 和 `phone_number_otp` 两个参数。
phone_number_otp_token	String	发送短信验证码成功后服务端返回的 `otp_token`。
phone_number_otp	String	用户手机收到的 OTP 验证码。
email	String	用户的邮箱地址。传递此参数时，须同时传递 `email_otp_token` 和 `email_otp` 两个参数。
email_otp_token	String	发送邮箱验证码成功后服务端返回的 `otp_token`。
email_otp	String	用户邮箱收到的 OTP 验证码。
name	String	用户姓名。
nickname	String	用户昵称。
zoneinfo	String	用户时区，如 `Asia/Shanghai` 或 `Europe/Paris`。
locale	String	用户 locale 信息，如 `zh-CN` 或 `en-US`。

说明：

其他参数的取值为用户属性标识。属性标识可以在 属性自定义页面 的属性详情界面查看。

正常响应示例



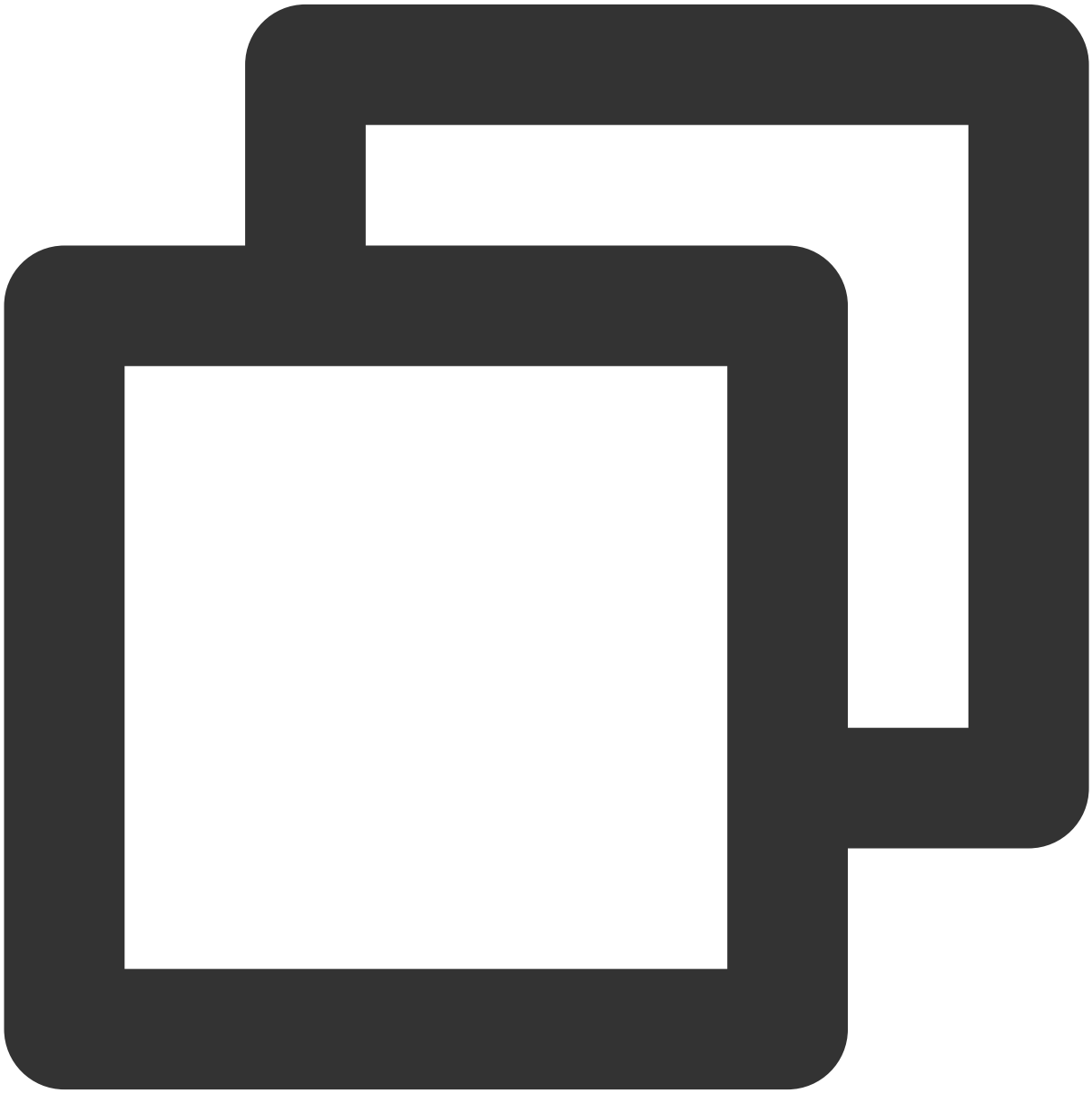
```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "sub" : "MOCK_USER_ID",
  "email" : "MOCK_USERNAME@example.com",
  "name" : "MOCK_NAME",
  "nickname" : "MOCK_NICKNAME",
  "zoneinfo" : "Asia/Shanghai",
  "locale" : "zh-CN"
}
```

说明：

除 `sub` 字段一定返回外，其余返回哪些字段由应用参数配置中的 `Claims` 决定。

异常响应示例

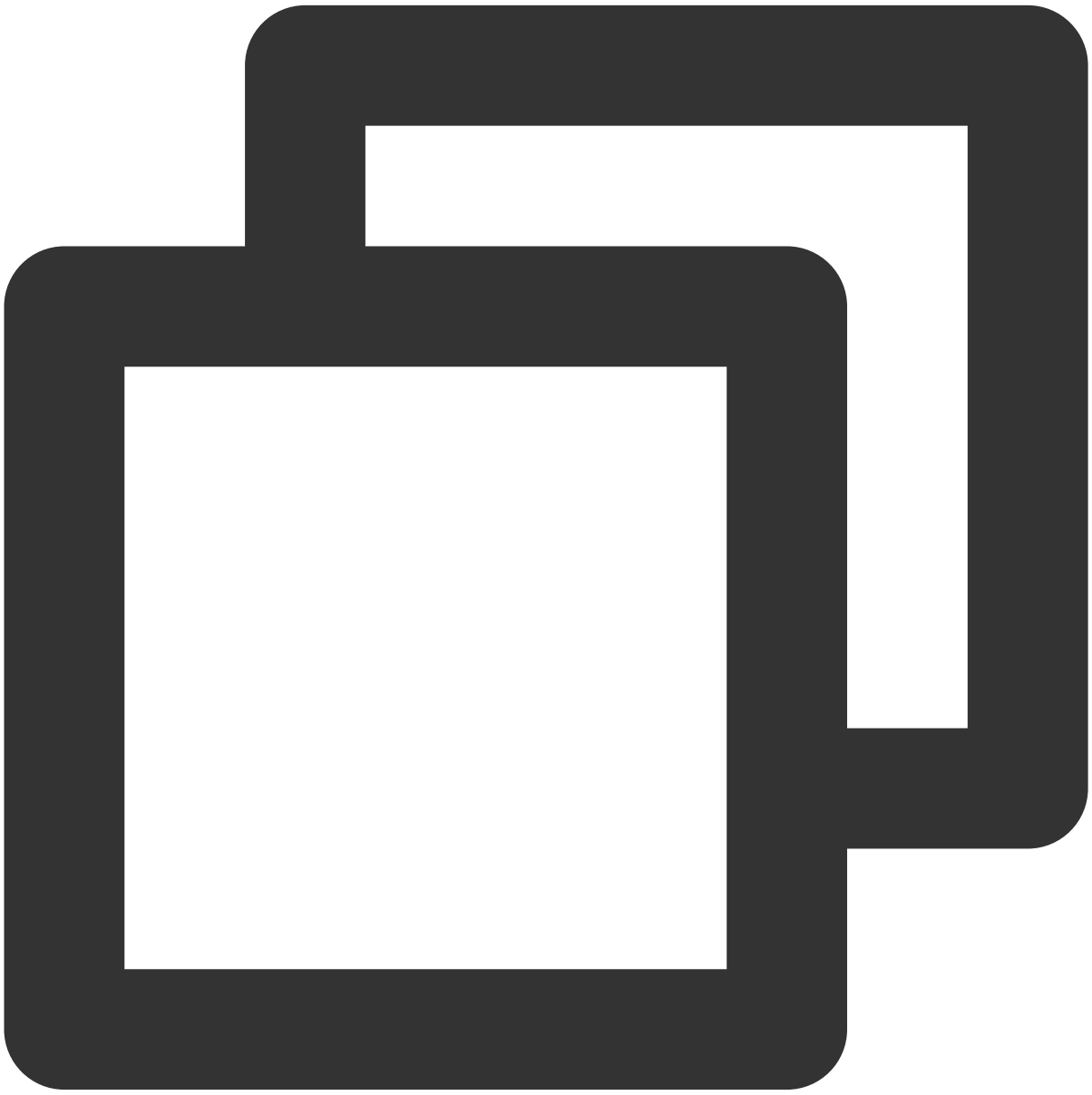
入参包含未知属性。



```
HTTP/1.1 400 Bad Request
```

```
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_request",
"error_description" : "Unknown attribute(s) found."
}
```

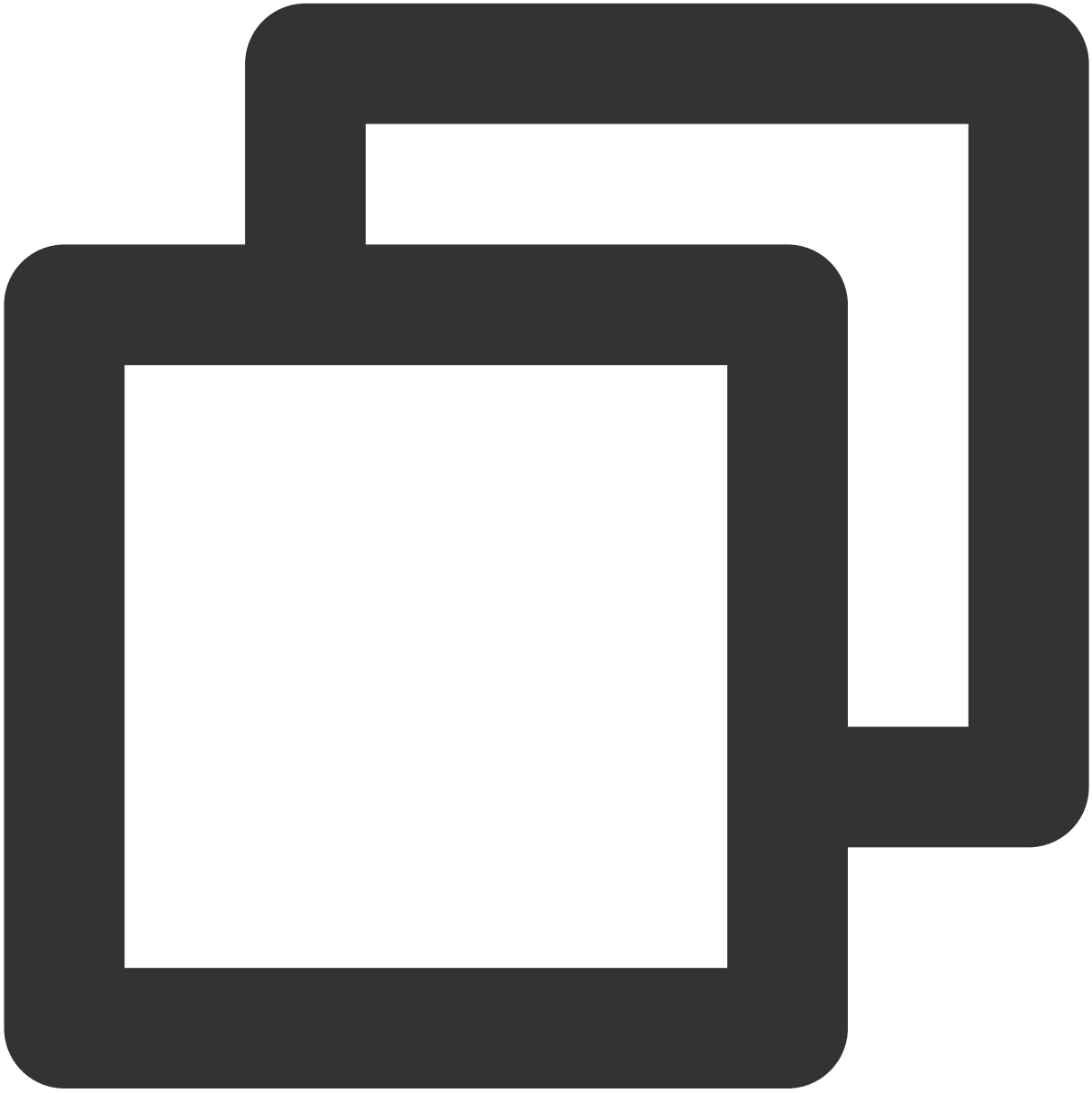
入参包含不支持修改的属性。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
```

```
{
"error" : "invalid_request",
"error_description" : "Unsupported user attribute(s) found."
}
```

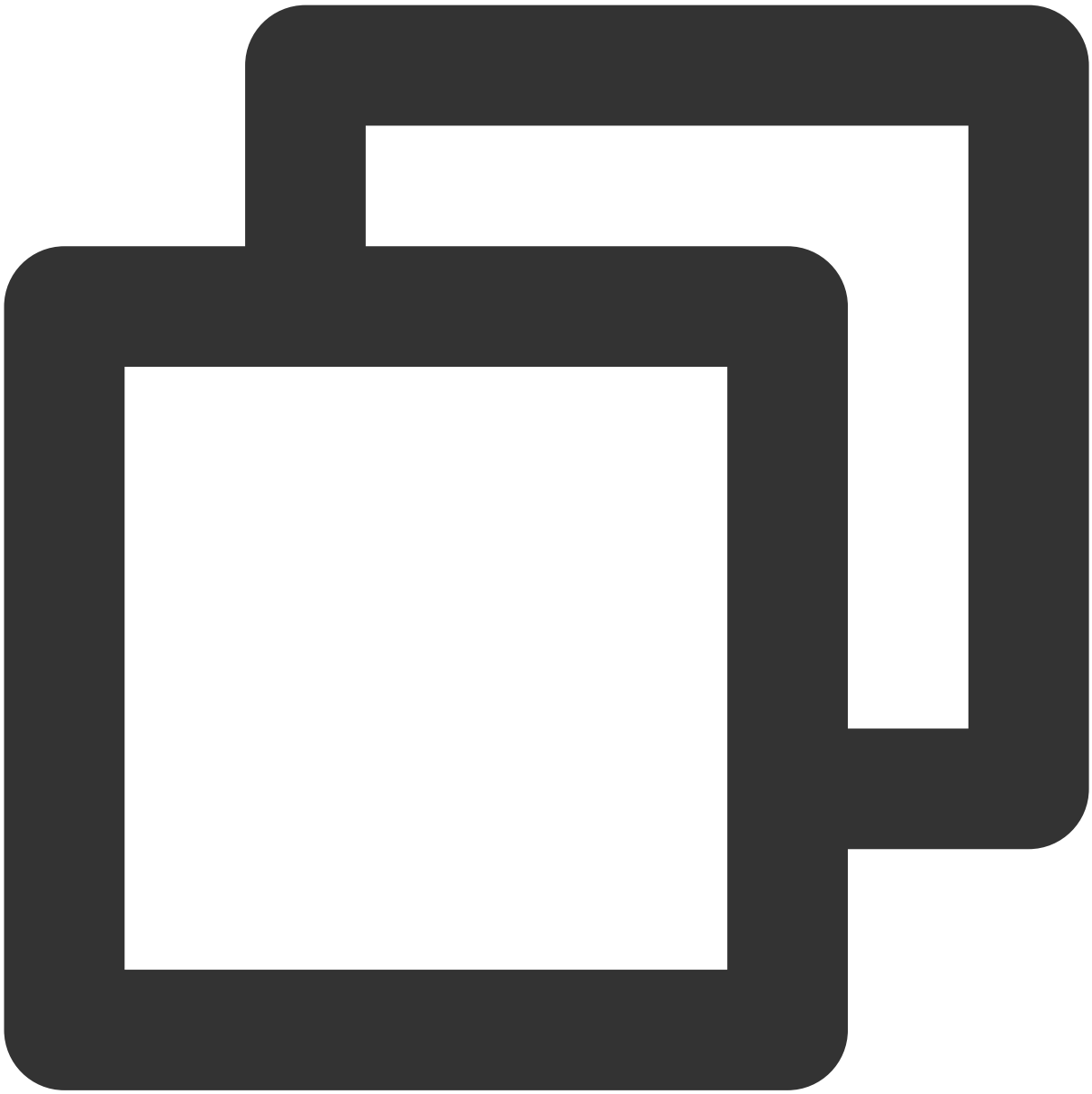
电话号码格式不合法。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "malformed_phone_number"
```

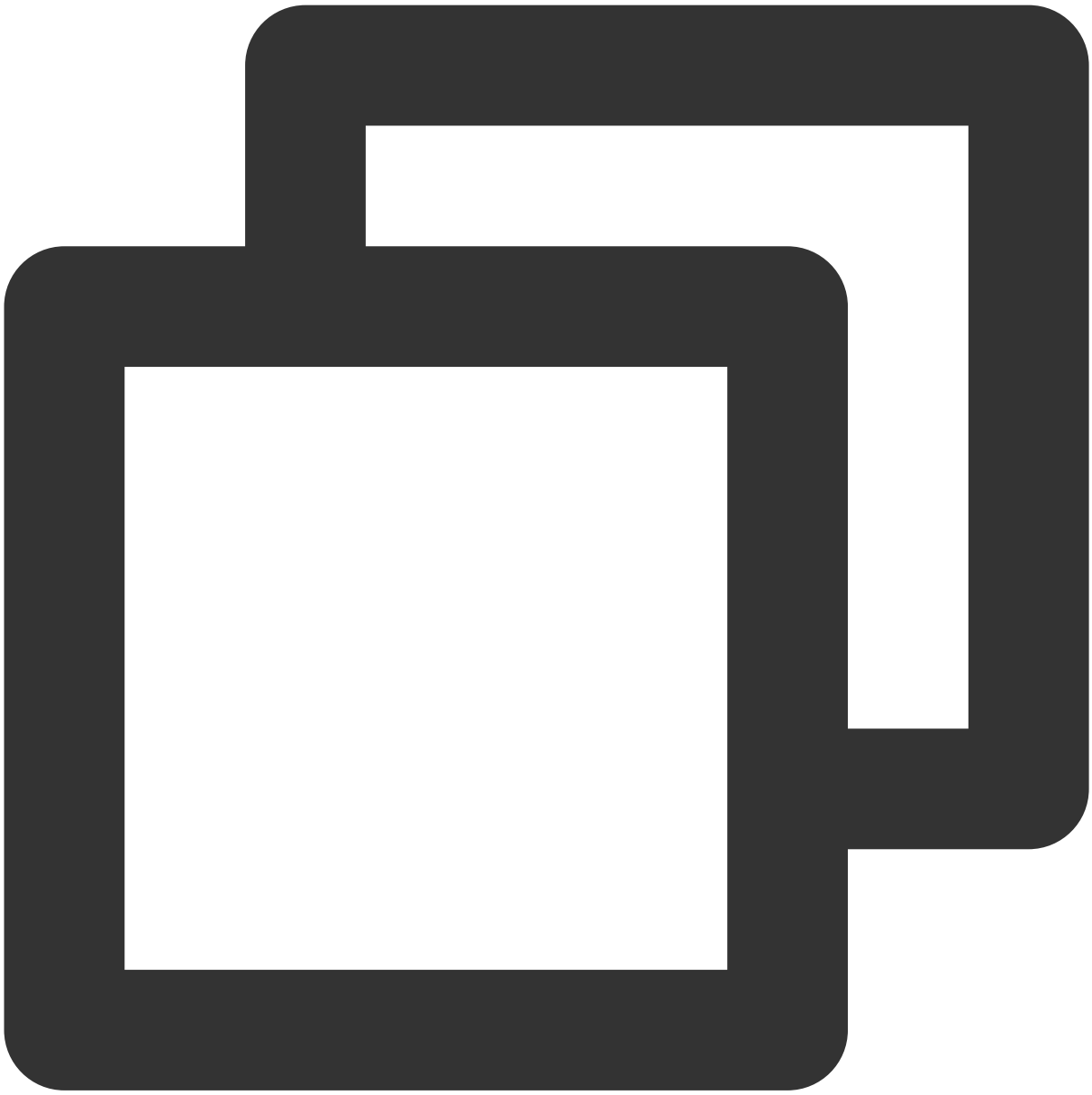
```
}
```

电话号码已存在。



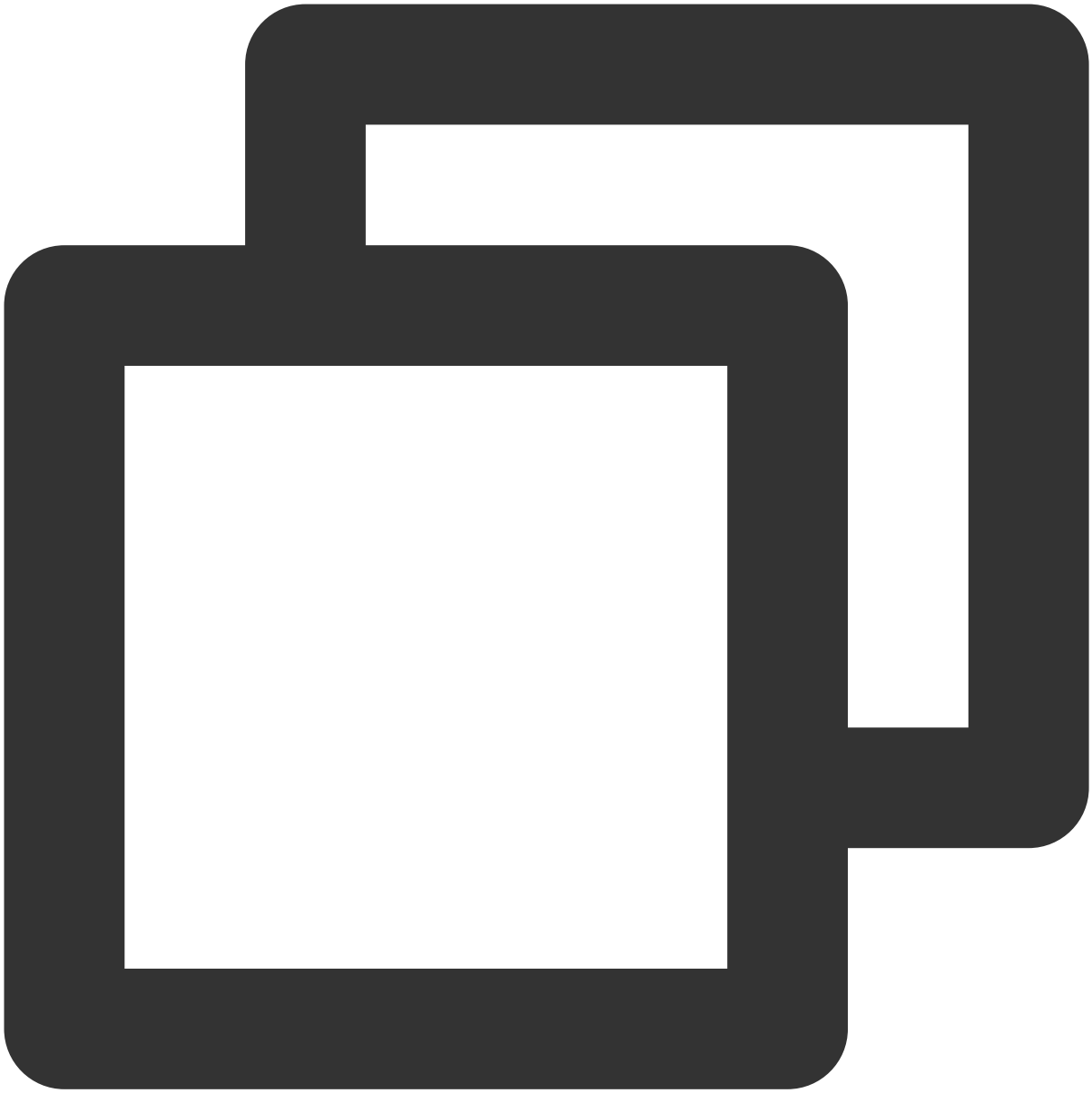
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_phone_number"
}
```

`phone_number_otp_token` 错误或已过期，或注册时使用的参数与发送验证码时不一致（例如：手机号不同）。



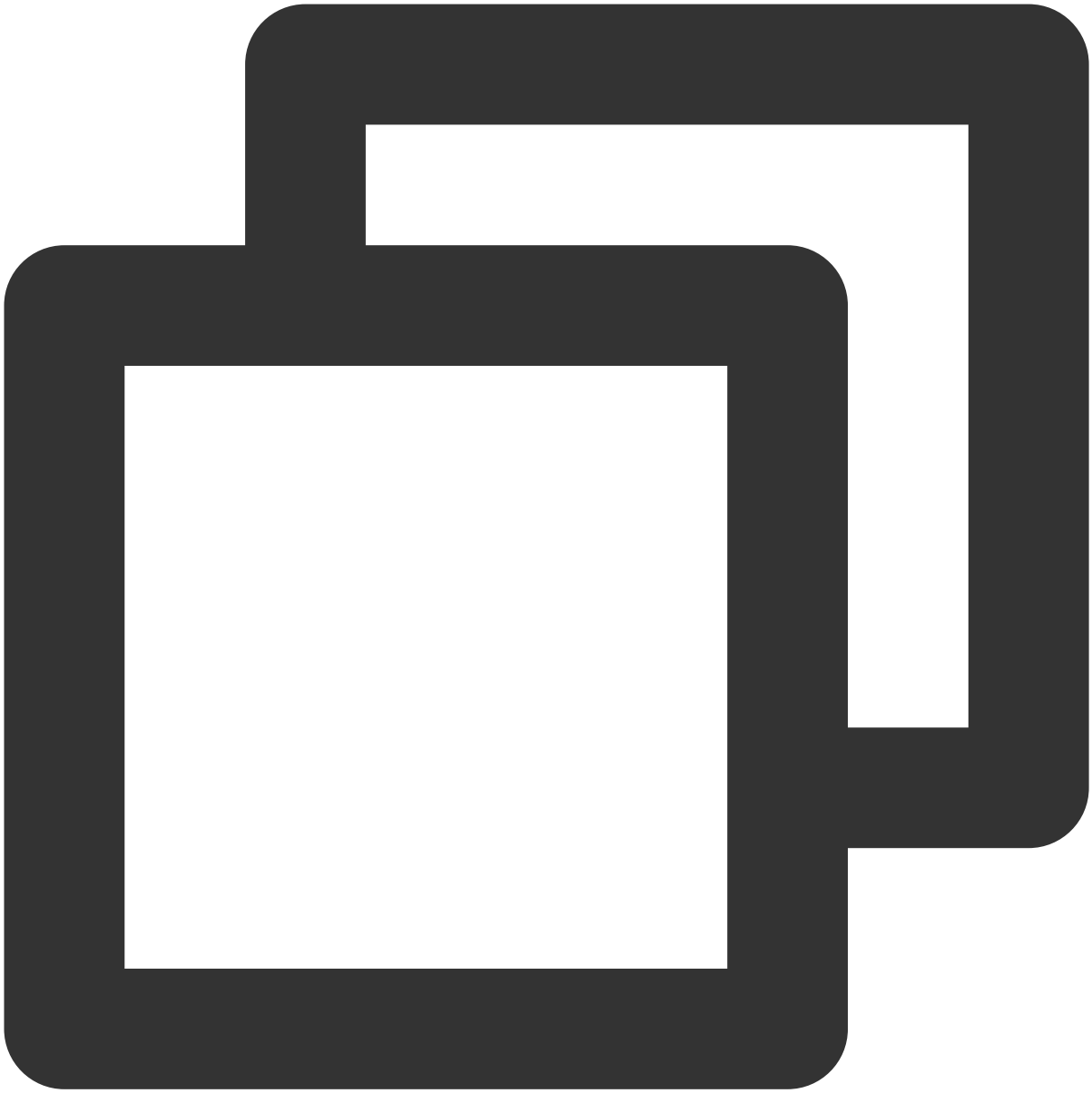
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_phone_number_otp_token"
}
```

`phone_number_otp` 错误或已过期。



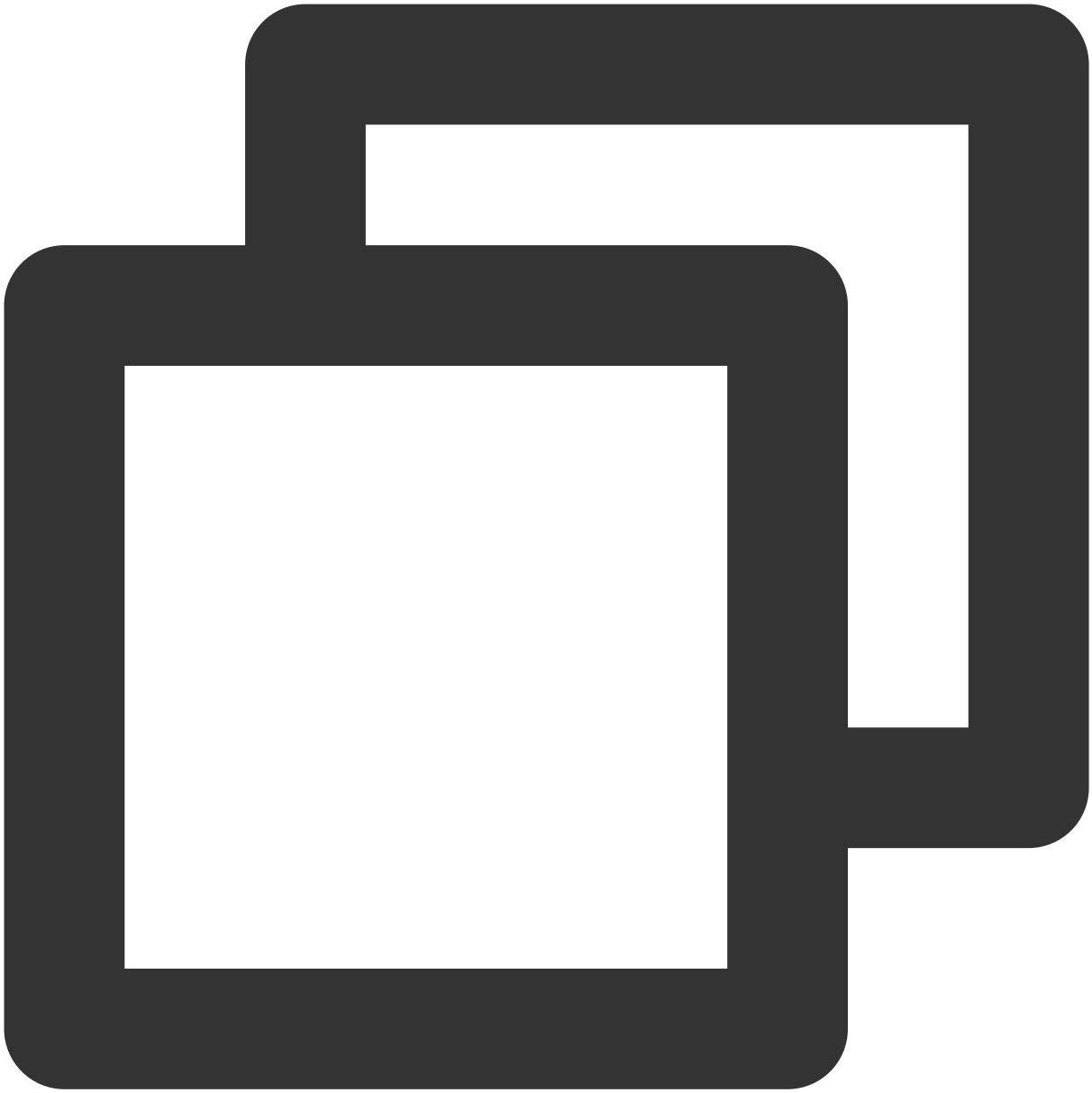
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_phone_number_otp"
}
```

邮箱格式不合法。



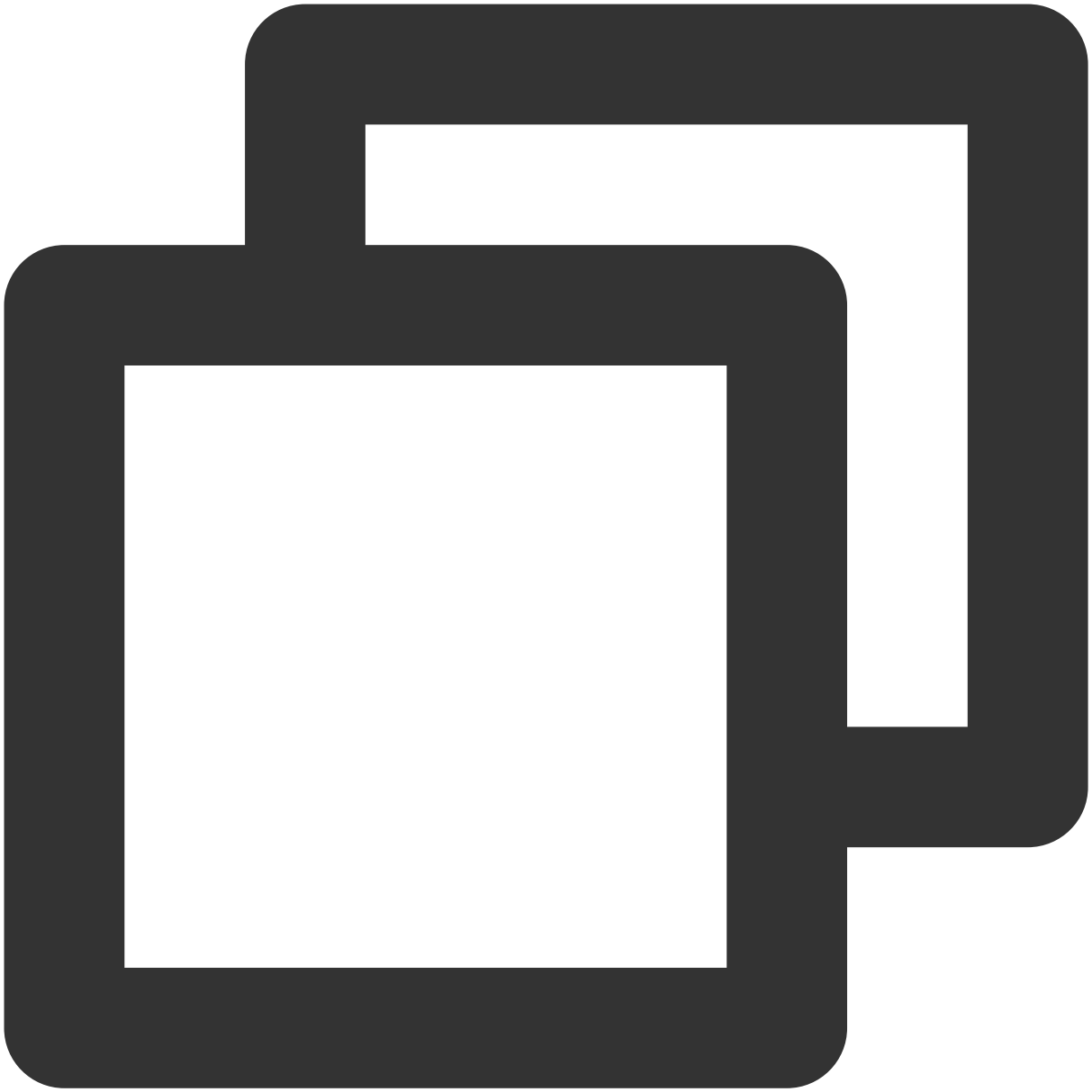
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "malformed_email"
}
```

邮箱已存在。



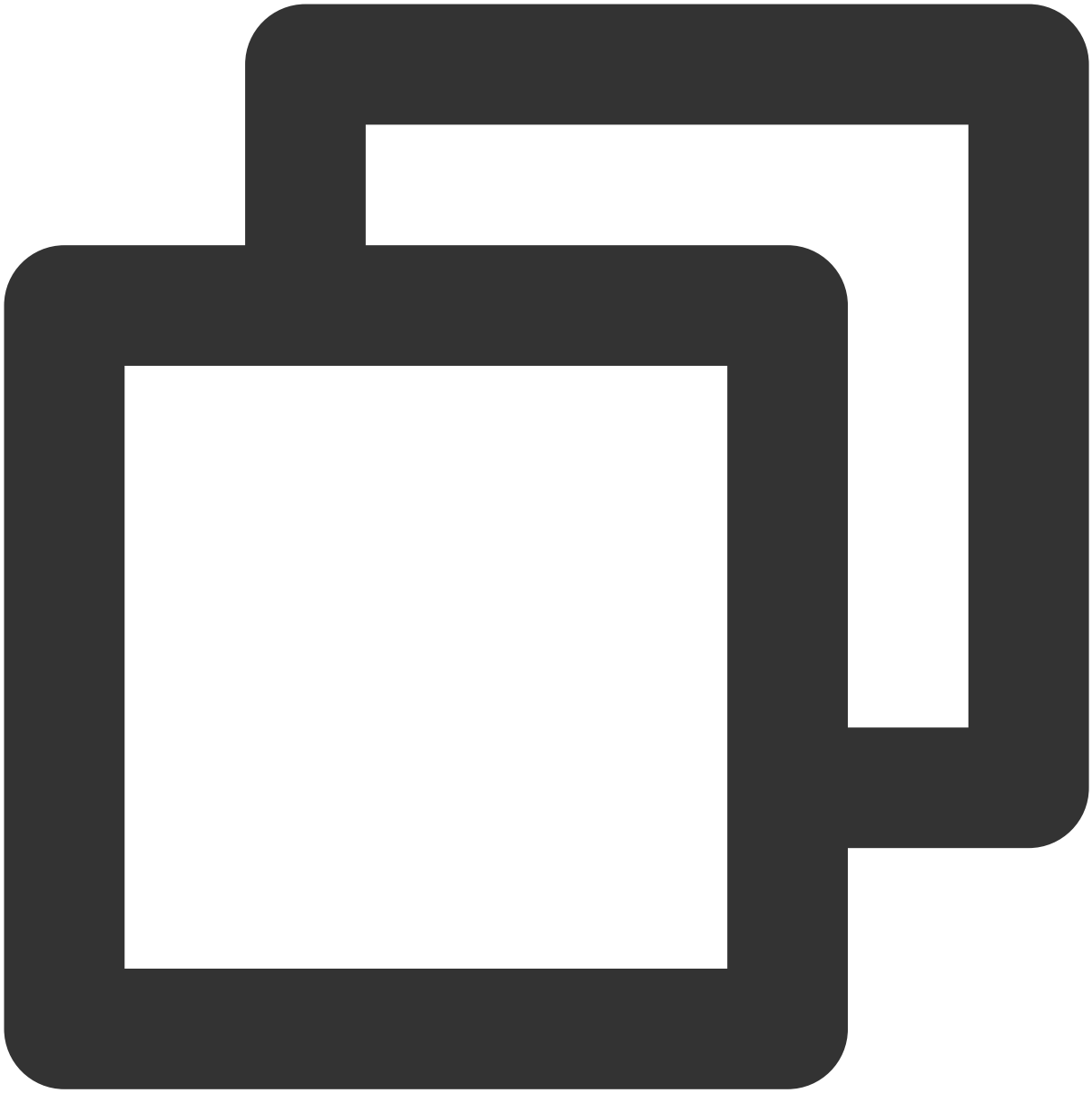
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_email"
}
```

`email_otp_token` 错误或已过期，或注册时使用的参数与发送验证码时不一致（例如：邮箱不同）。



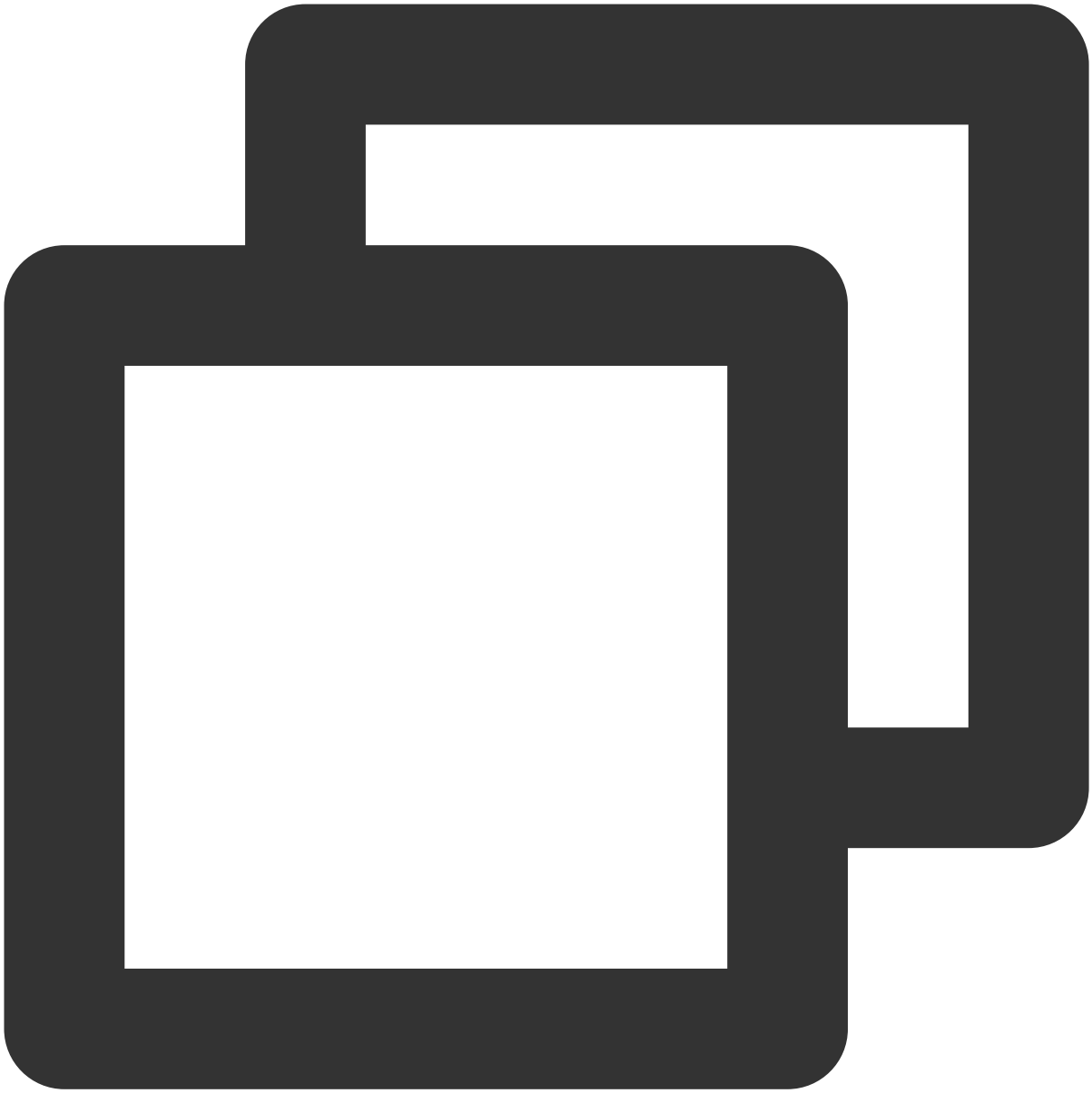
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp_token"
}
```

`email_otp` 错误或已过期。



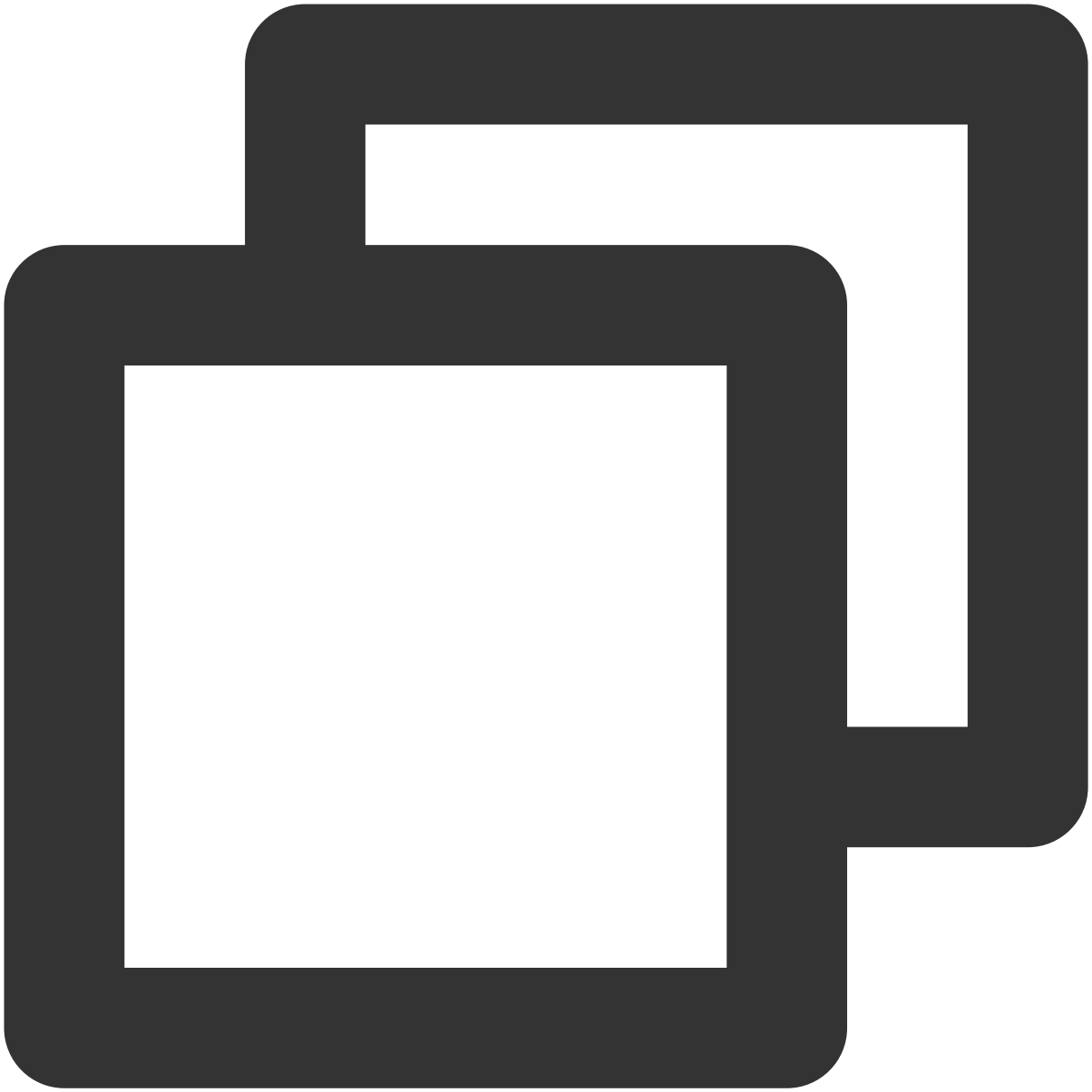
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp"
}
```

入参取值不合法（例如：不符合用户属性正则表达式）。



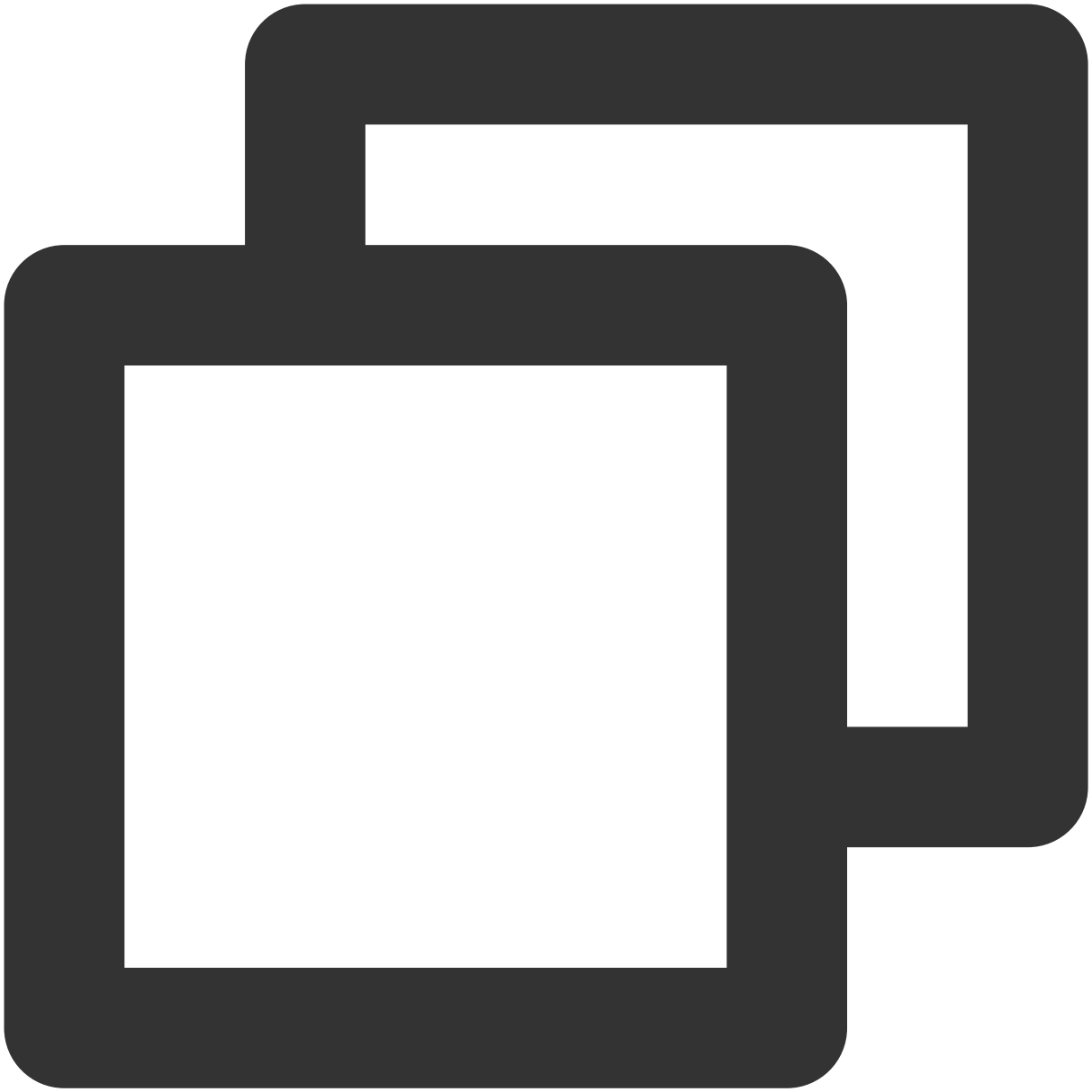
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "illegal_parameter_value"
}
```

`bearer_token` 缺失。



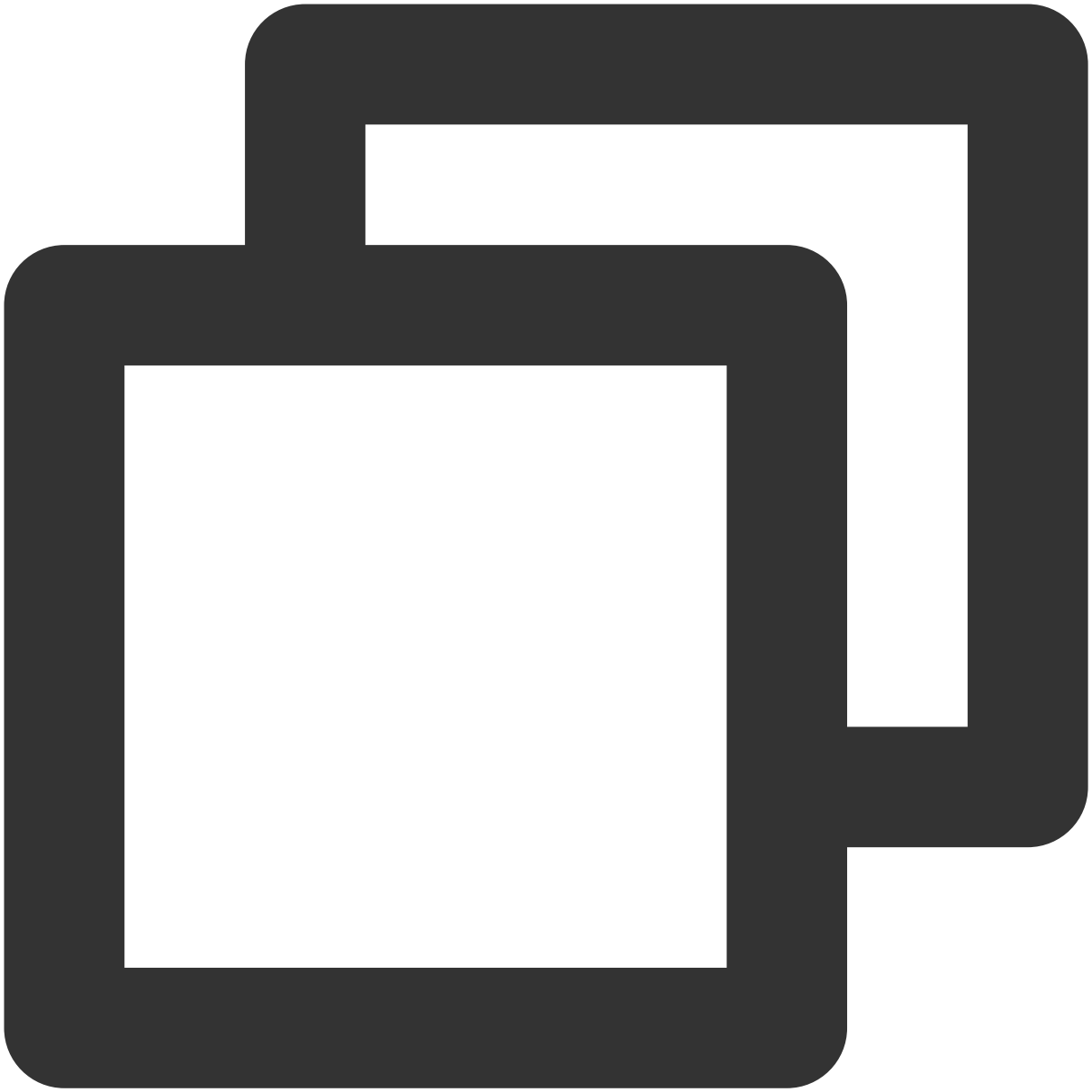
```
HTTP/1.1 400 Bad Request
WWW-Authenticate: Bearer error="invalid_request", error_description="Bearer token n
```

`bearer_token` 错误。



```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="invalid_token", error_description="Error decoding J
```

`bearer_token` 无效。



```
HTTP/1.1 403 Forbidden
WWW-Authenticate: Bearer error="insufficient_scope", error_description="The request
```

修改用户密码

最近更新时间：2023-12-22 11:42:07

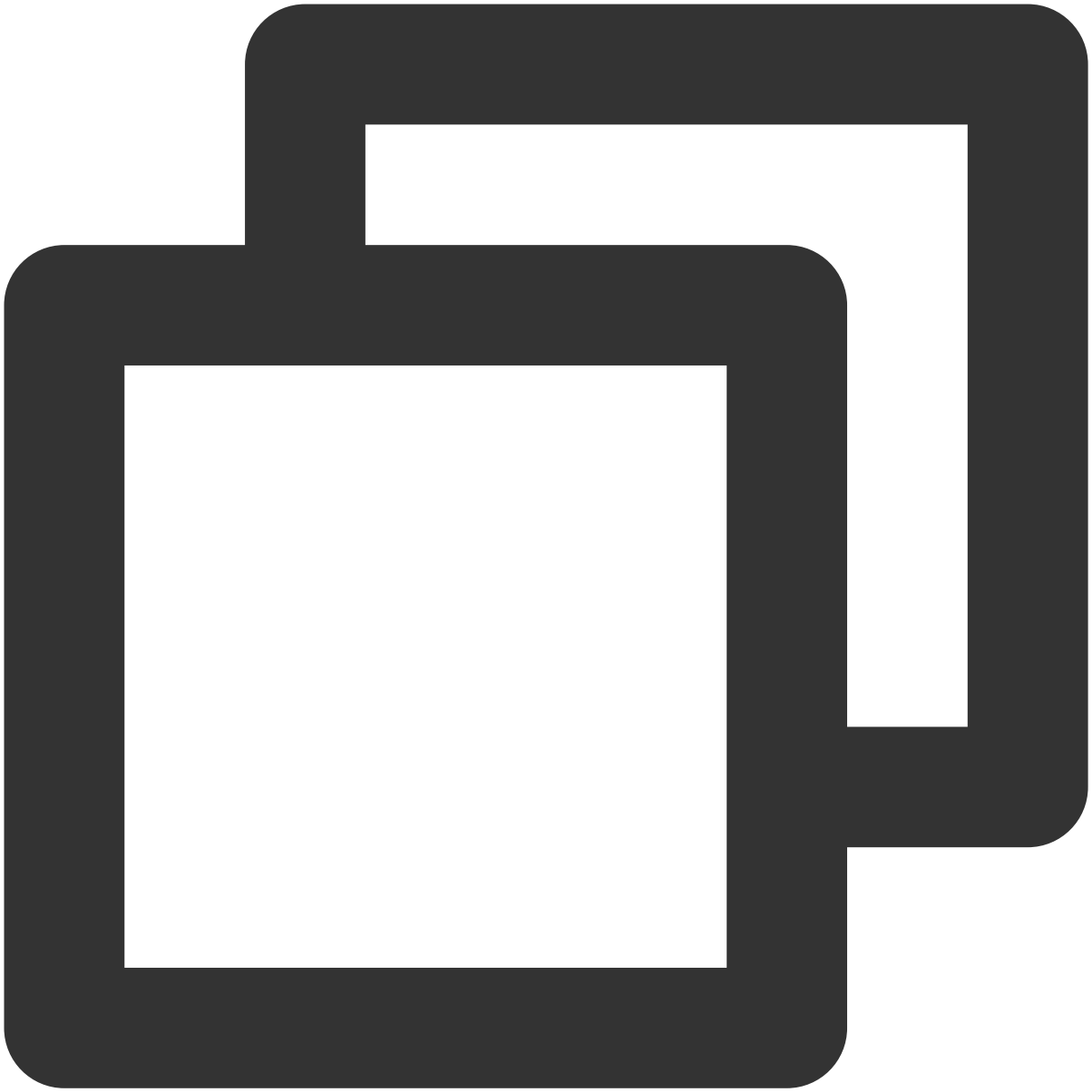
接口描述

修改已登录用户的密码。调用此接口时，需携带登录成功时得到的具备 `openid scope 的 Access Token` 。新密码需符合当前应用关联的账号密码认证源的密码策略，且不能与策略中指定的前 N 次历史密码相同。

支持的应用类型

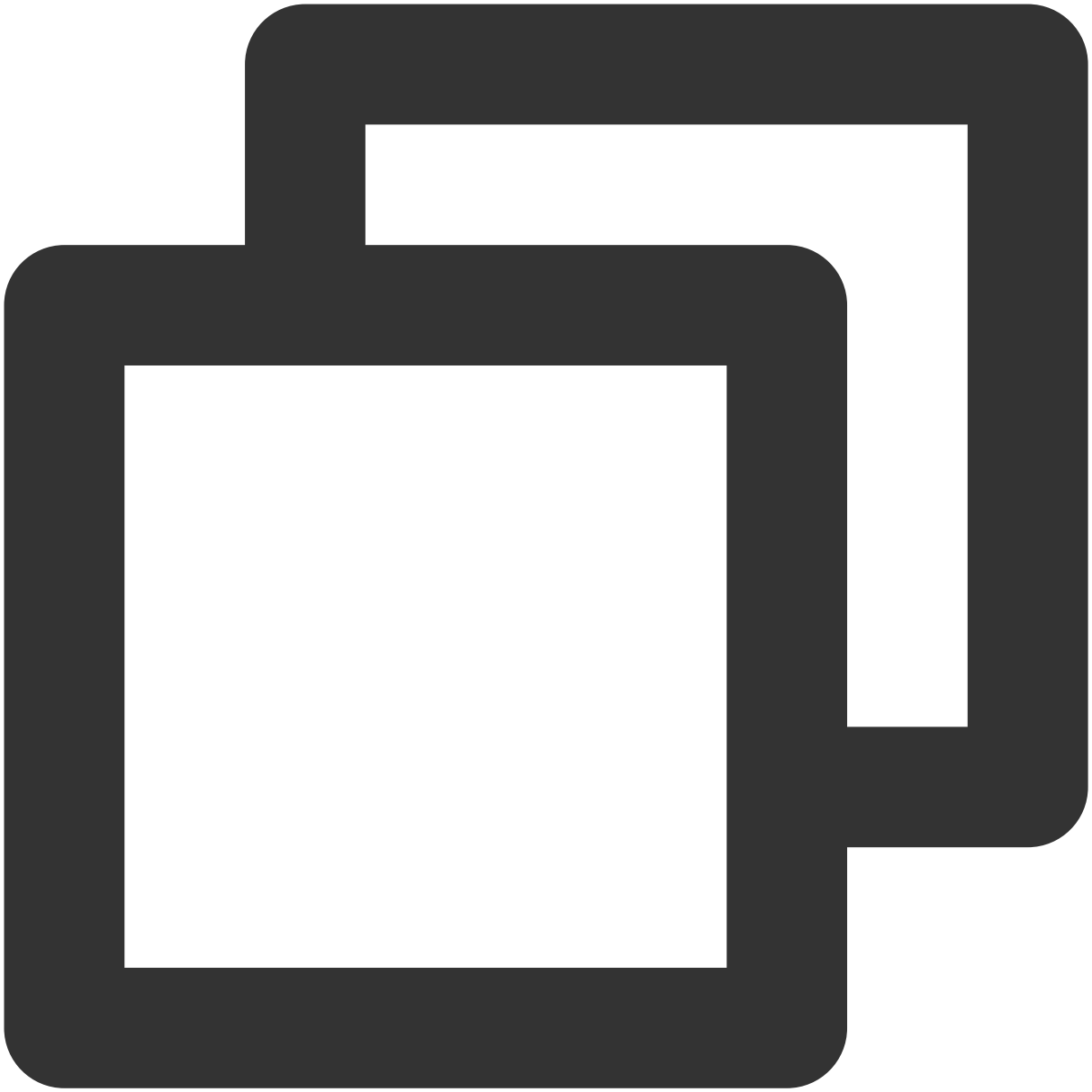
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



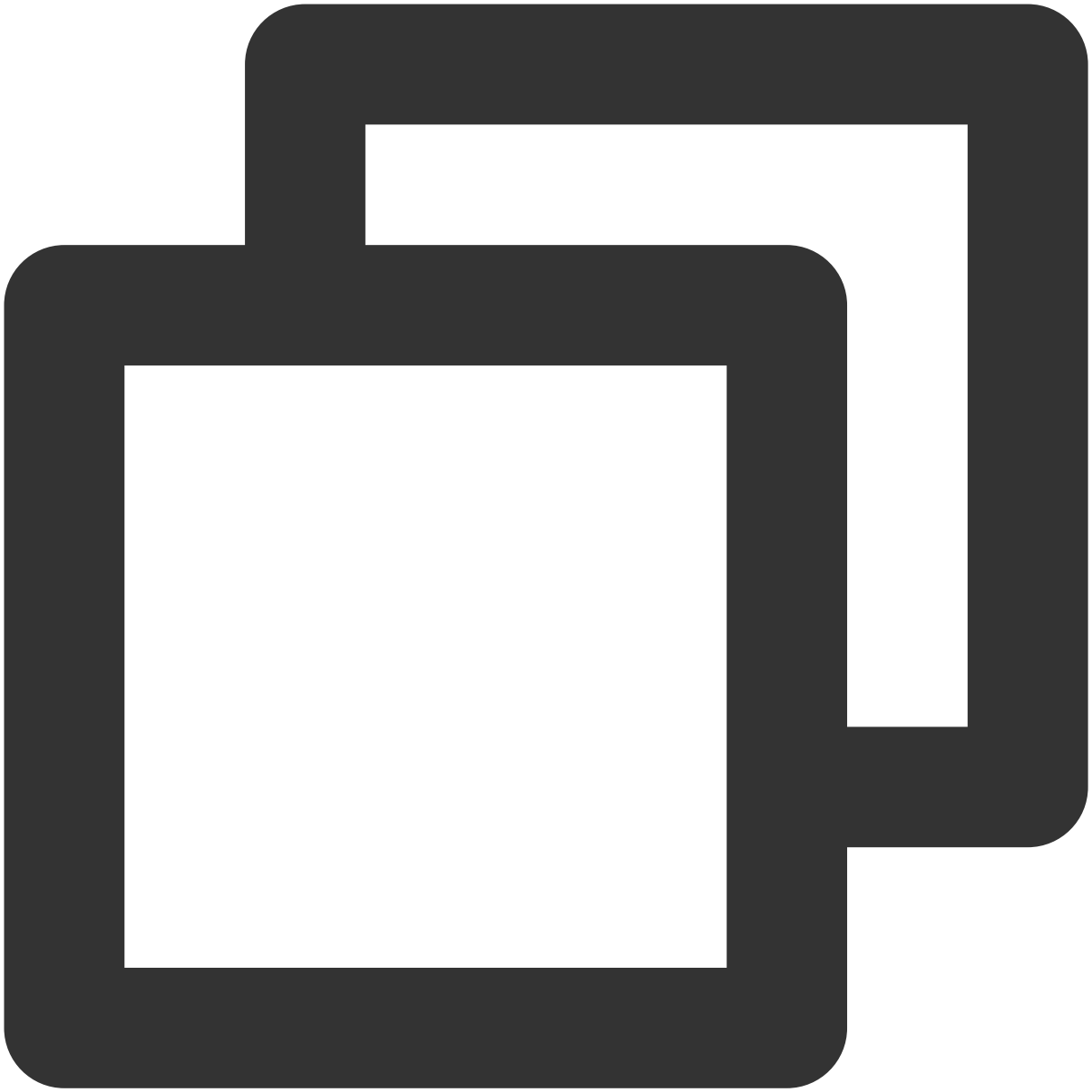
```
POST
```

请求路径



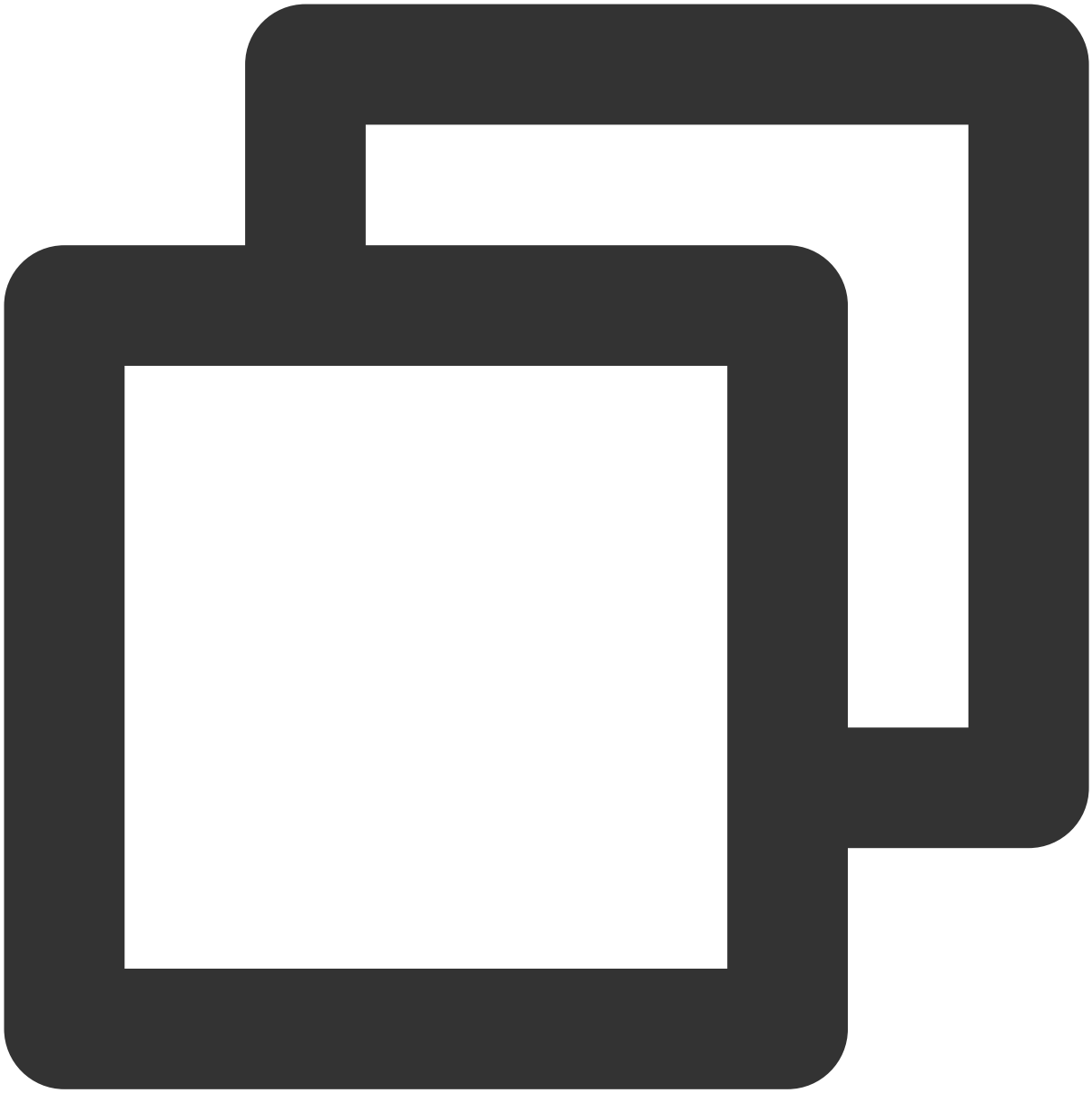
```
/change_user_password
```

请求 Content-Type



```
application/json
```

请求示例



```
POST /change_user_password HTTP/1.1
Content-Type: application/json
Authorization: Bearer ACCESS_TOKEN_WITH_OPENID_SCOPE
Host: sample.portal.tencentciam.com

{
  "old_password" : "MOCK_PASSWORD",
  "new_password" : "MOCK_NEW_PASSWORD"
}
```

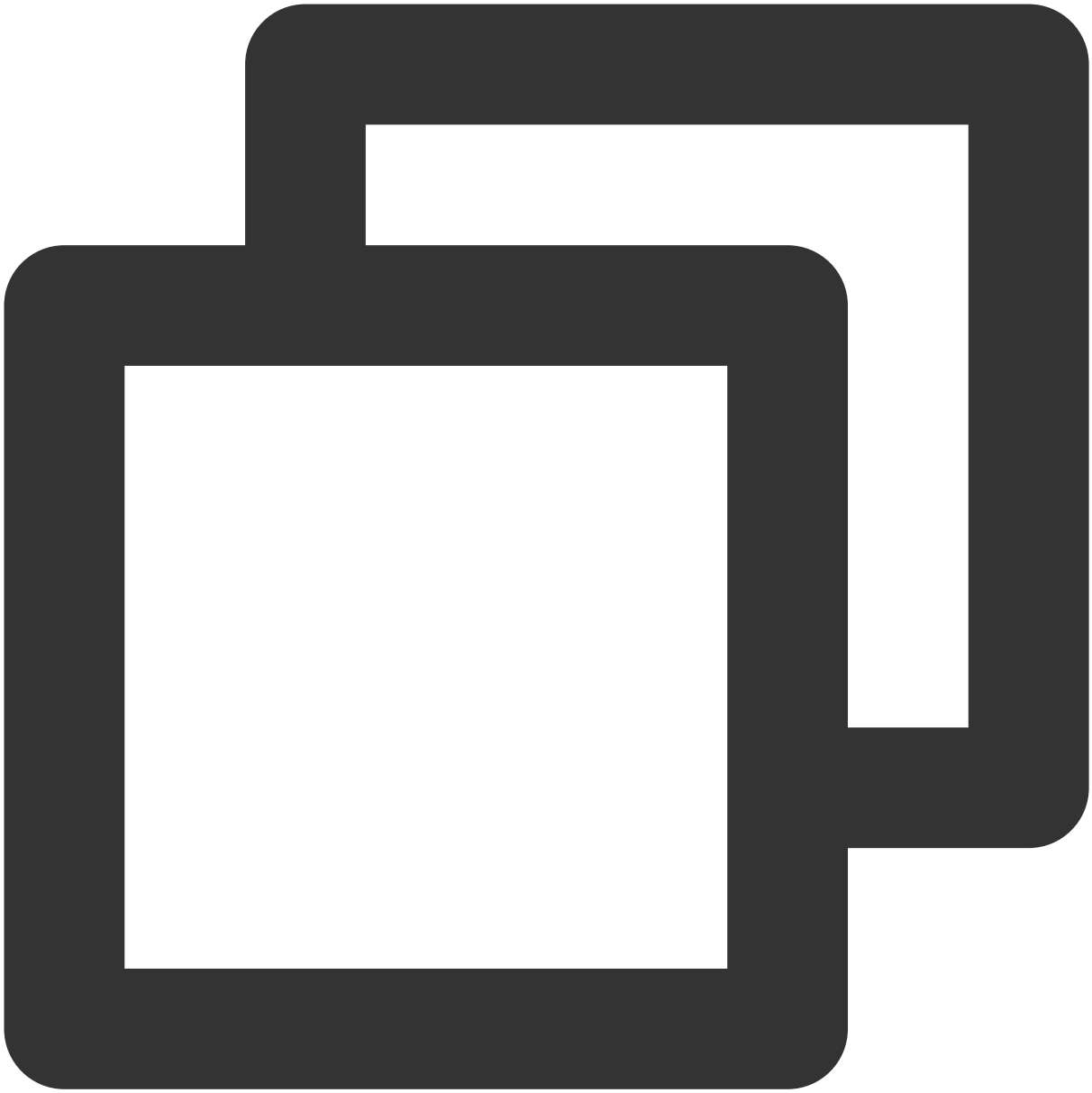
请求头

名称	描述
Authorization	OAuth 2.0 Bearer Token，格式为 `Bearer <Token>`，其中 `Bearer` 为固定字符串，`<Token>` 为用户登录成功时得到的具备 `openid scope` 的 `Access Token`，`Bearer` 和 `<Token>` 之间用一个空格隔开。

请求体 JSON 参数

JSON 路径	数据类型	描述
old_password	String	旧密码。
new_password	String	新密码。

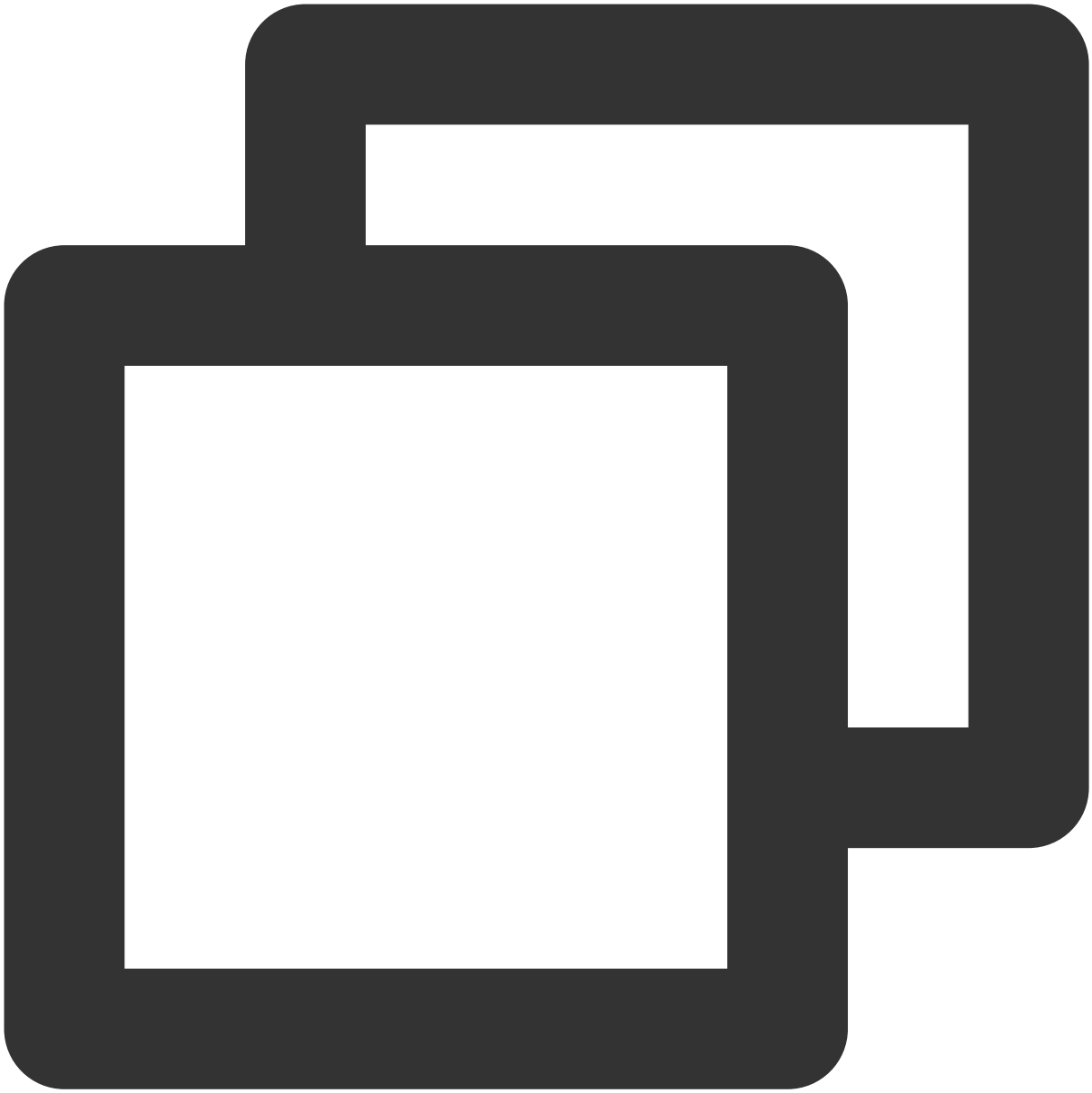
正常响应示例



```
HTTP/1.1 200 OK
```

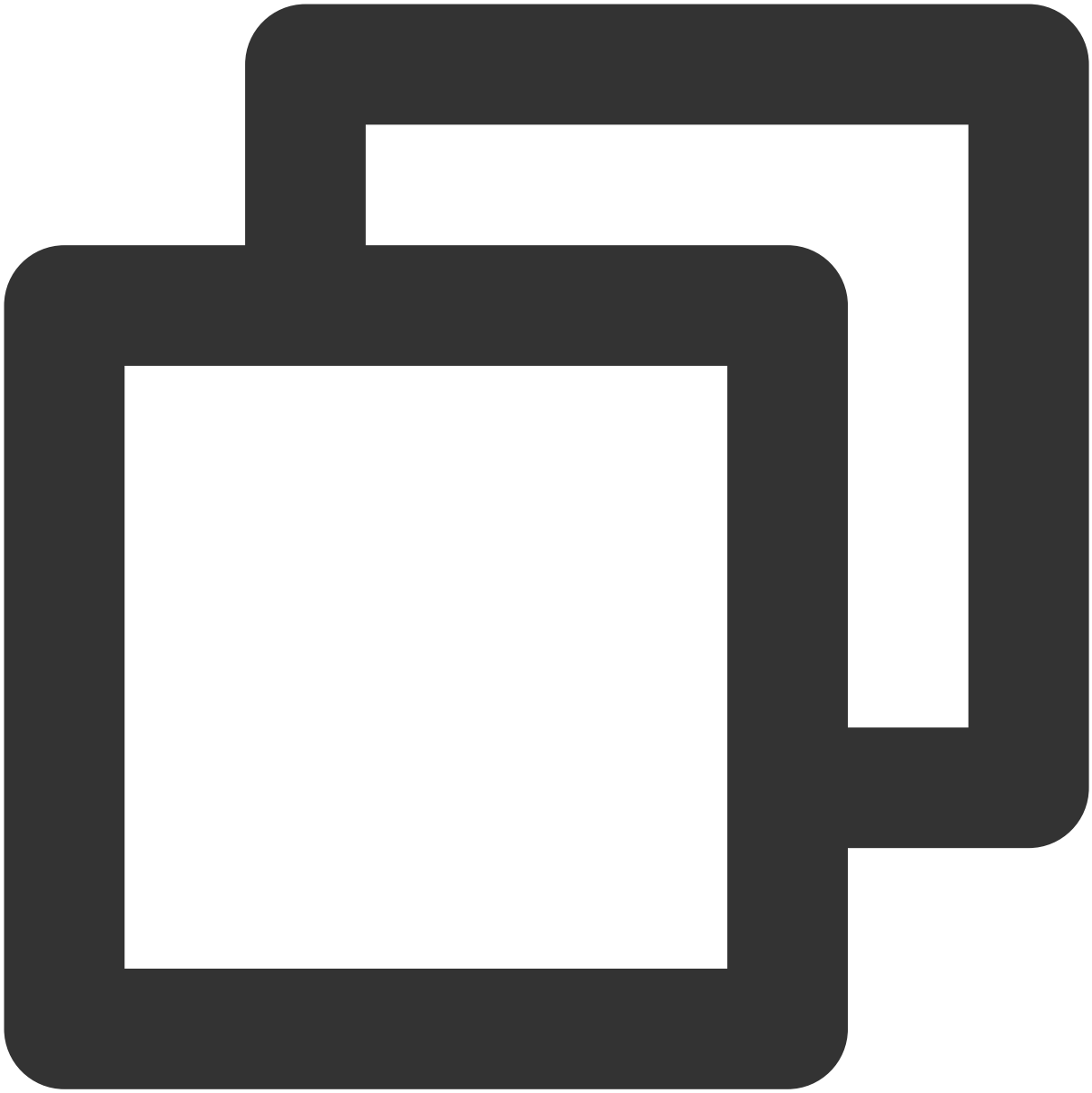
异常响应示例

旧密码错误。



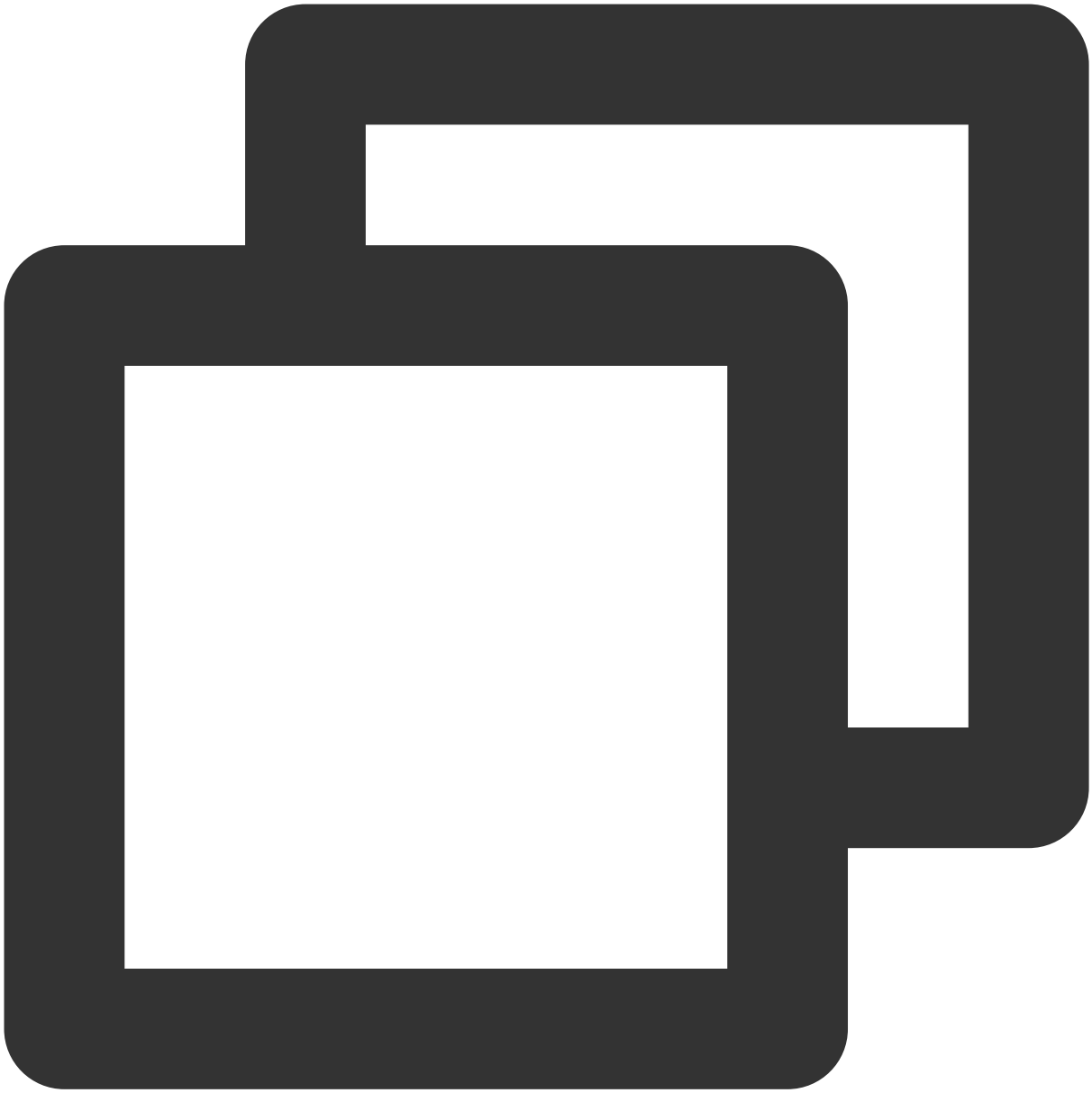
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "wrong_old_password"
}
```

新密码与旧密码相同。



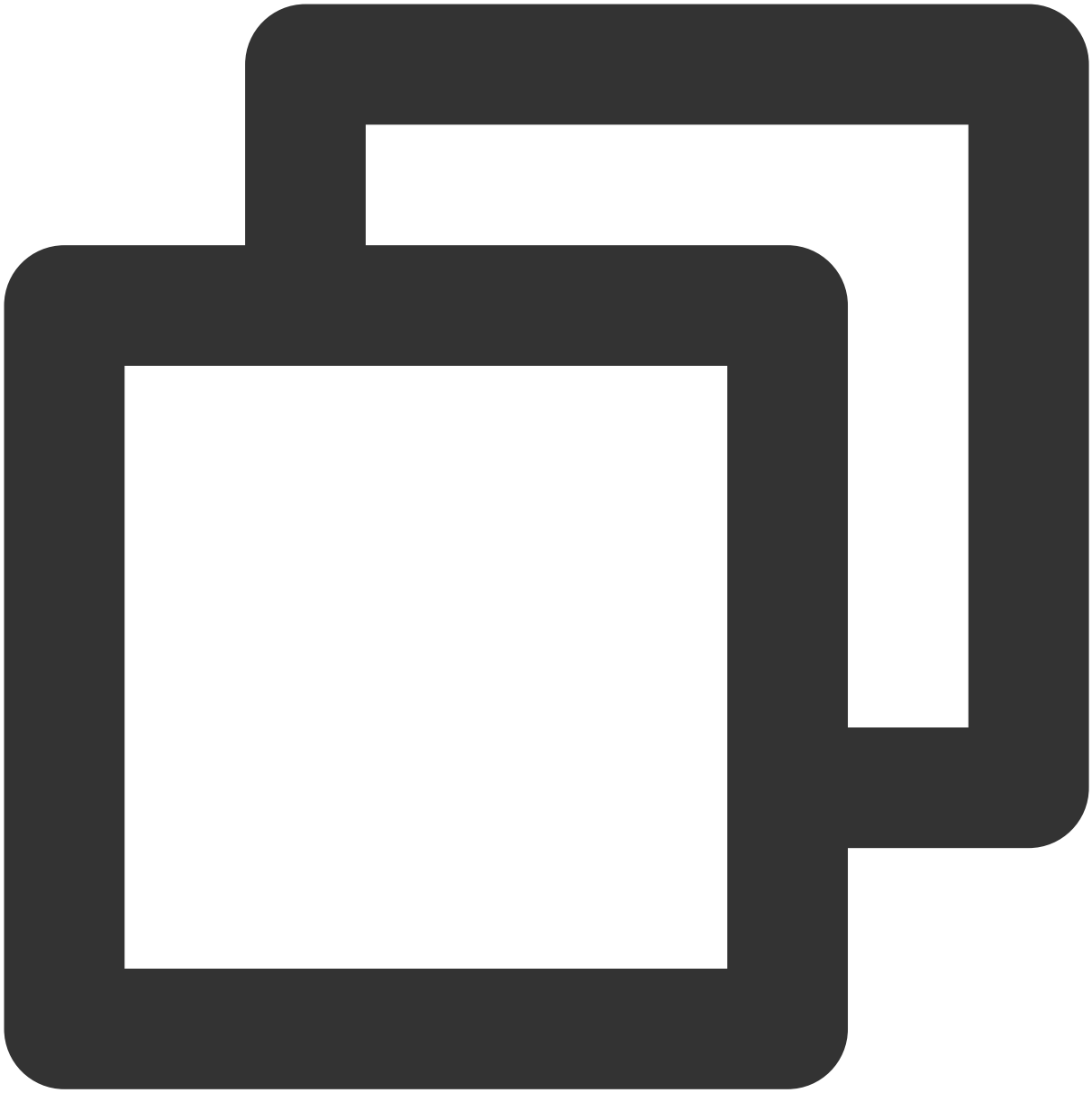
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "duplicate_password"
}
```

新密码与历史密码相同。



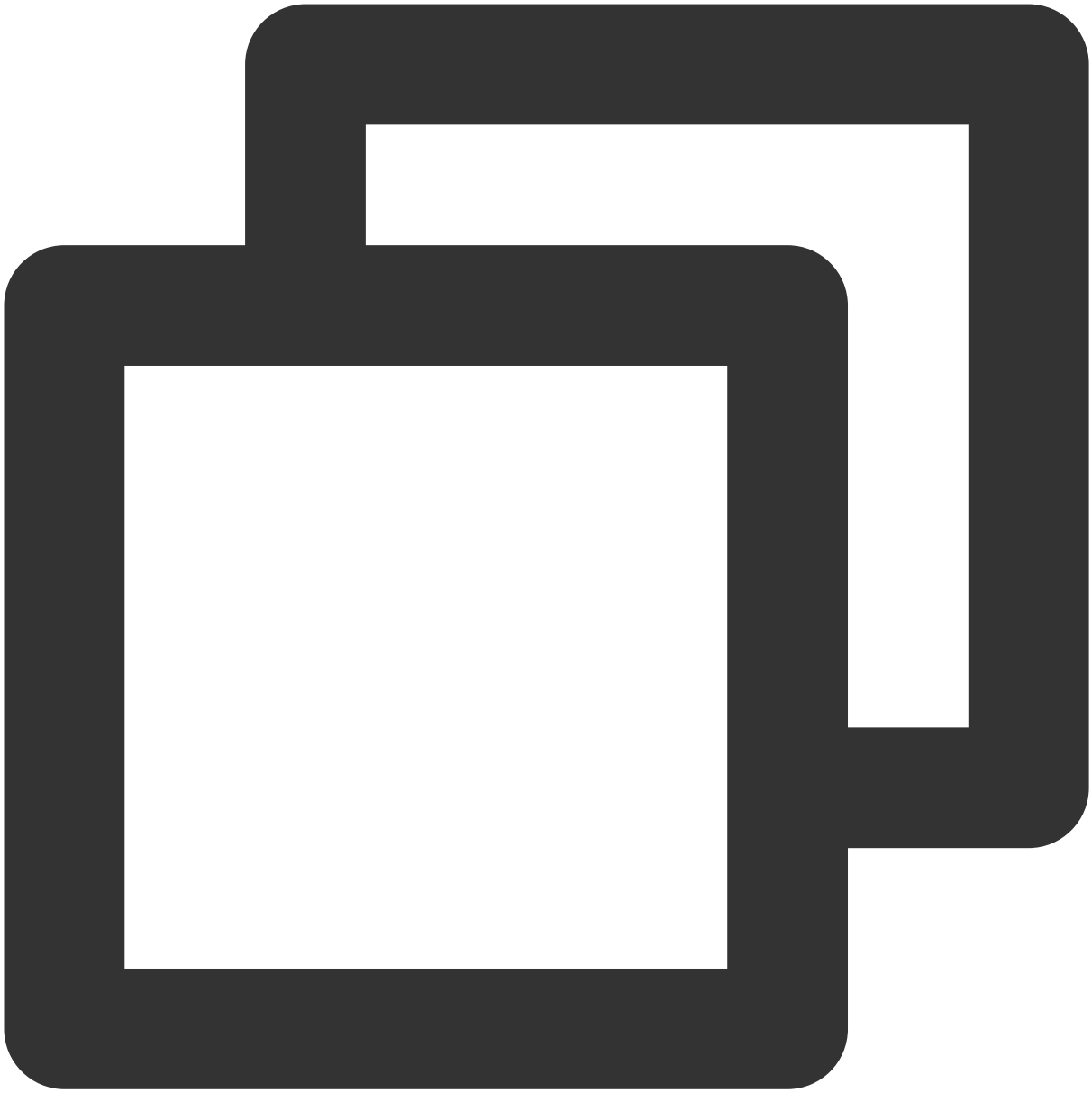
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "recurrent_password"
}
```

新密码不满足密码策略。



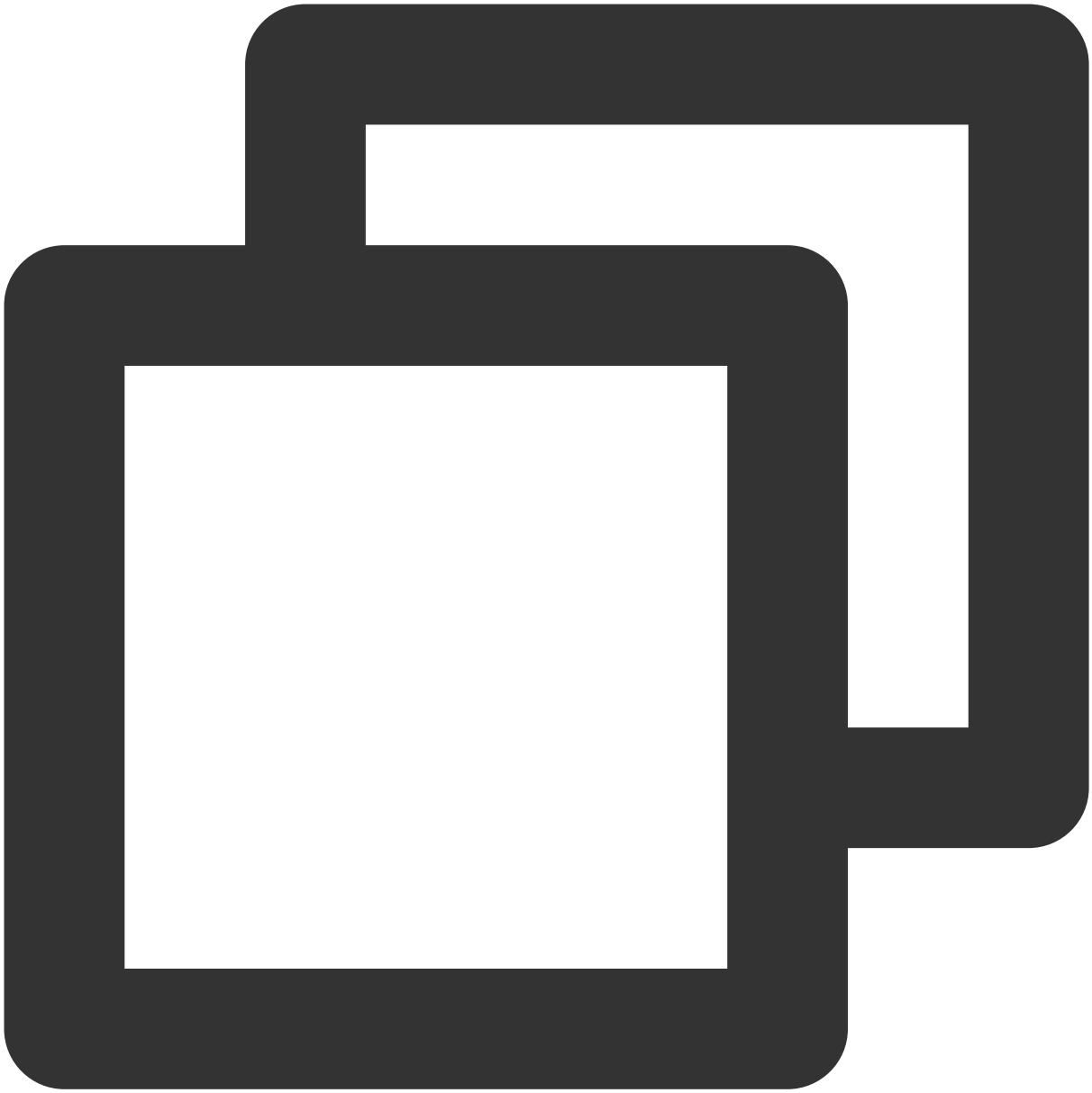
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_new_password"
}
```

用户未找到。



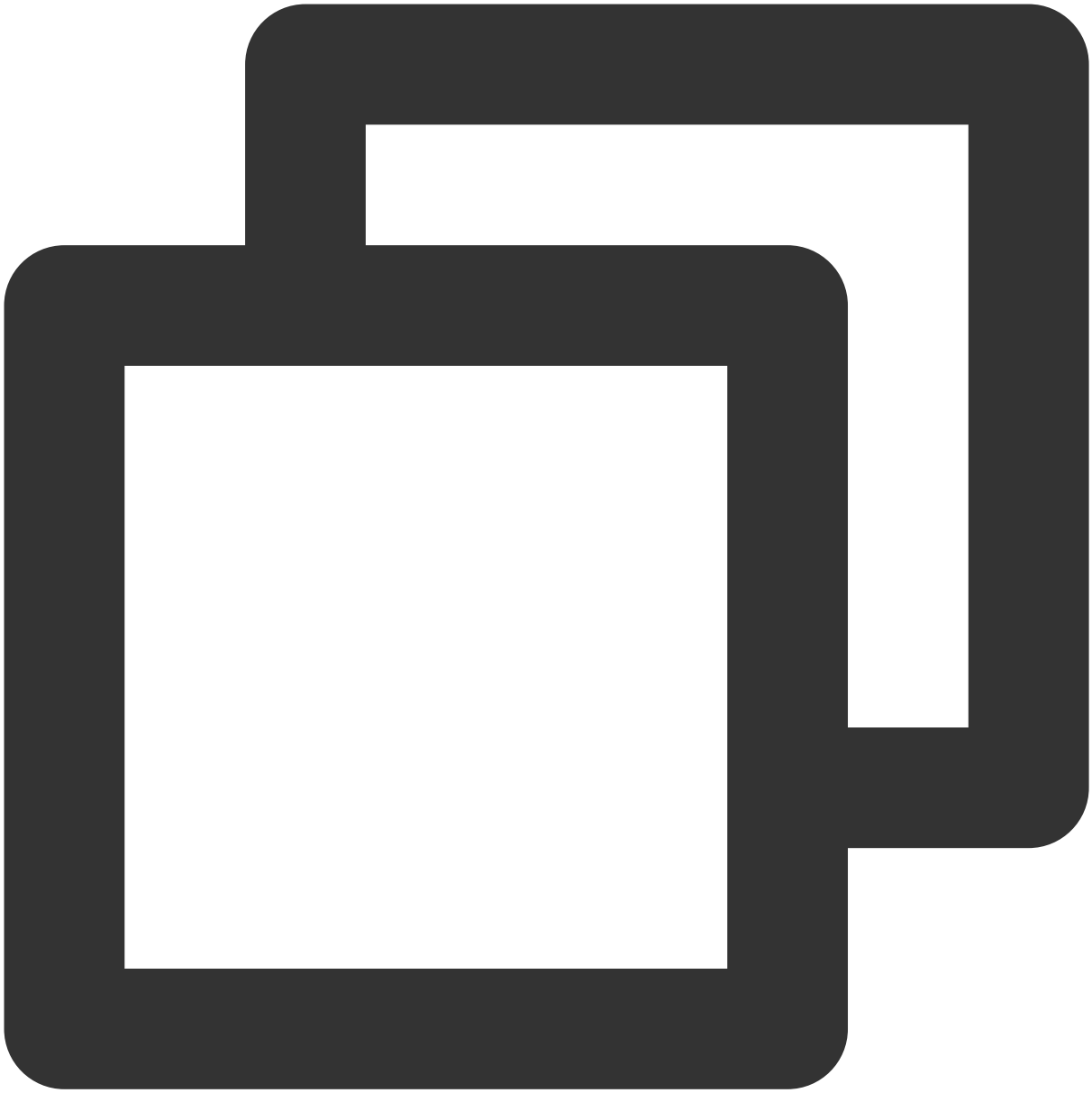
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "user_not_found"
}
```

用户被冻结。



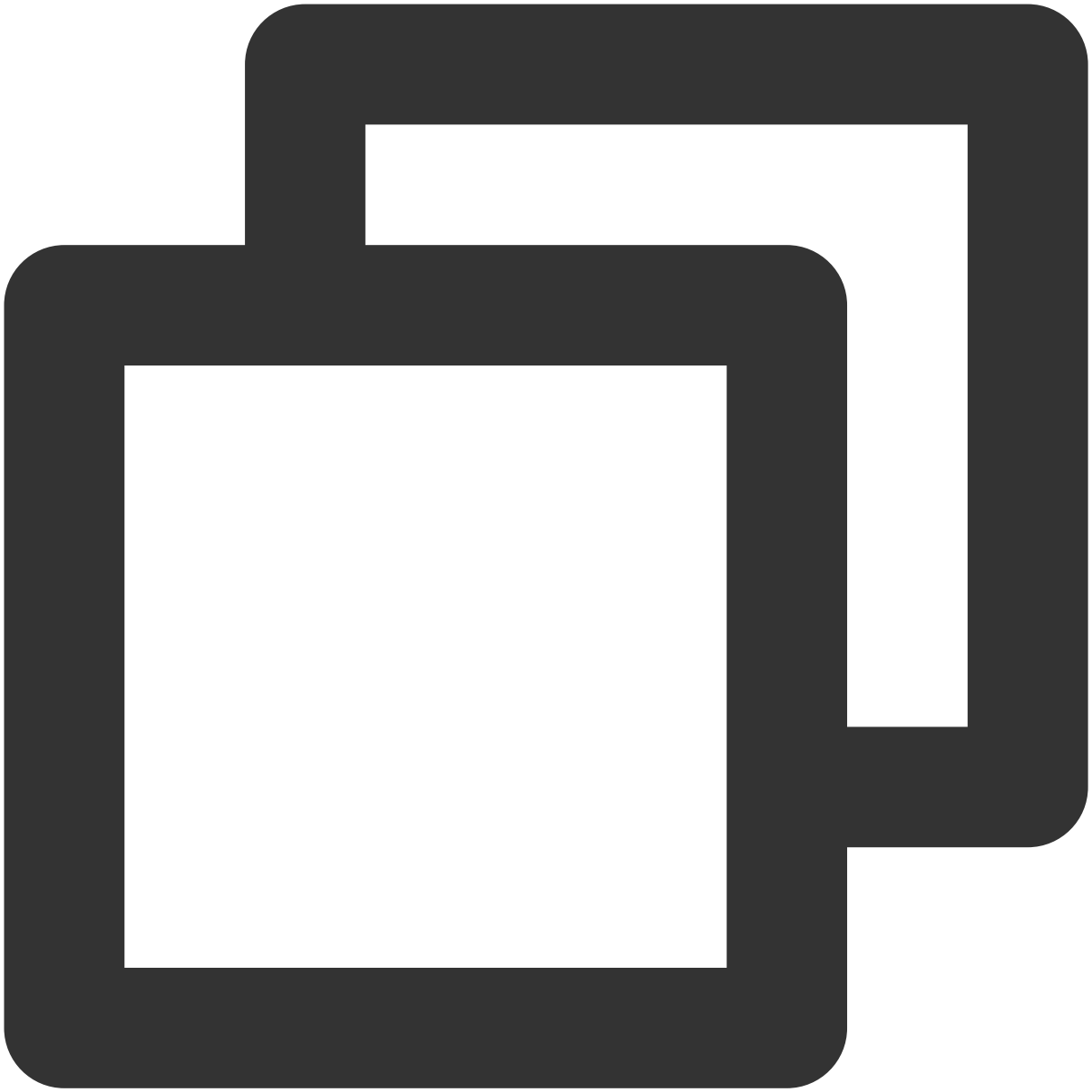
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "abnormal_user_status",
"error_description" : "User is frozen."
}
```

用户被锁定。



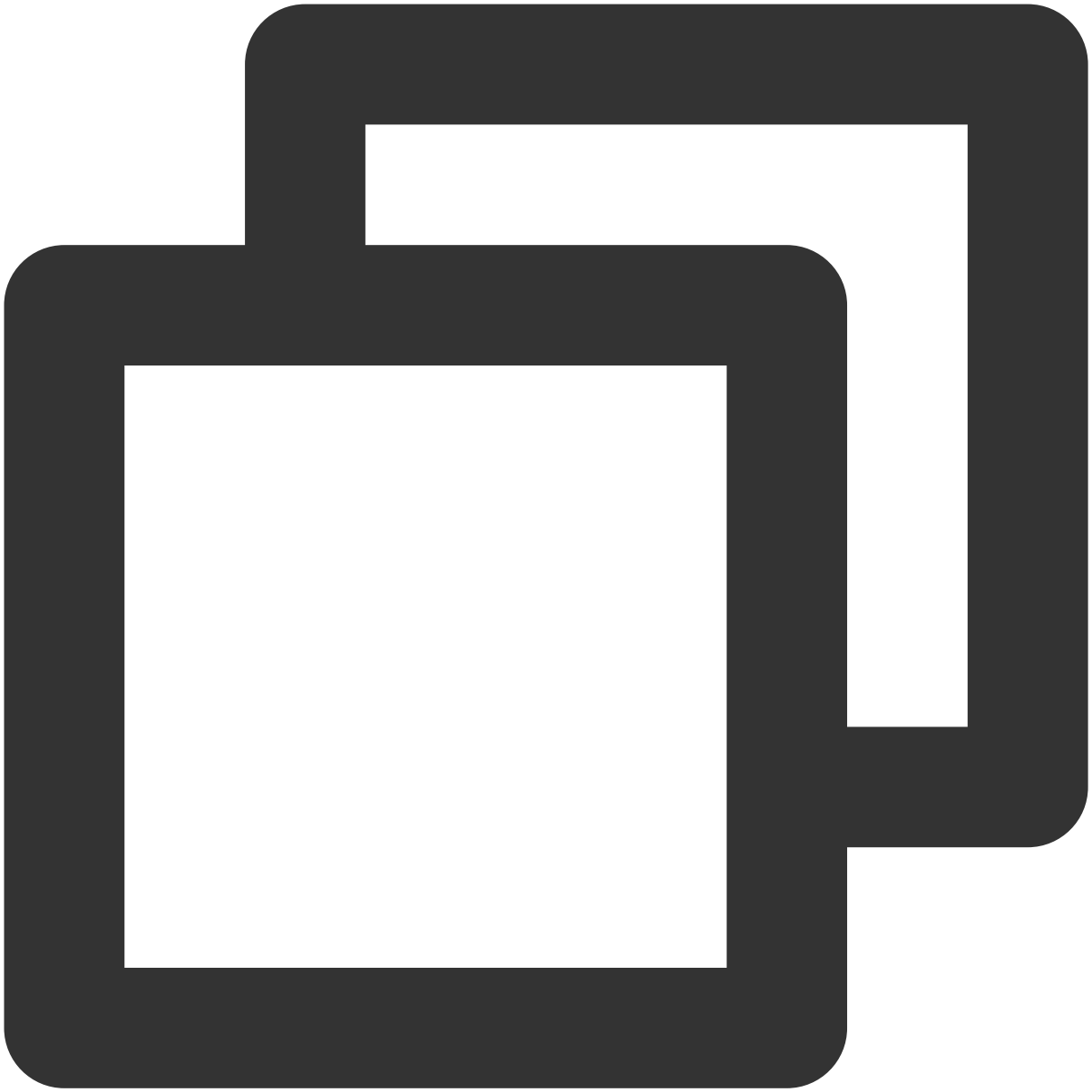
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "abnormal_user_status",
"error_description" : "User is locked."
}
```

`bearer_token` 缺失。



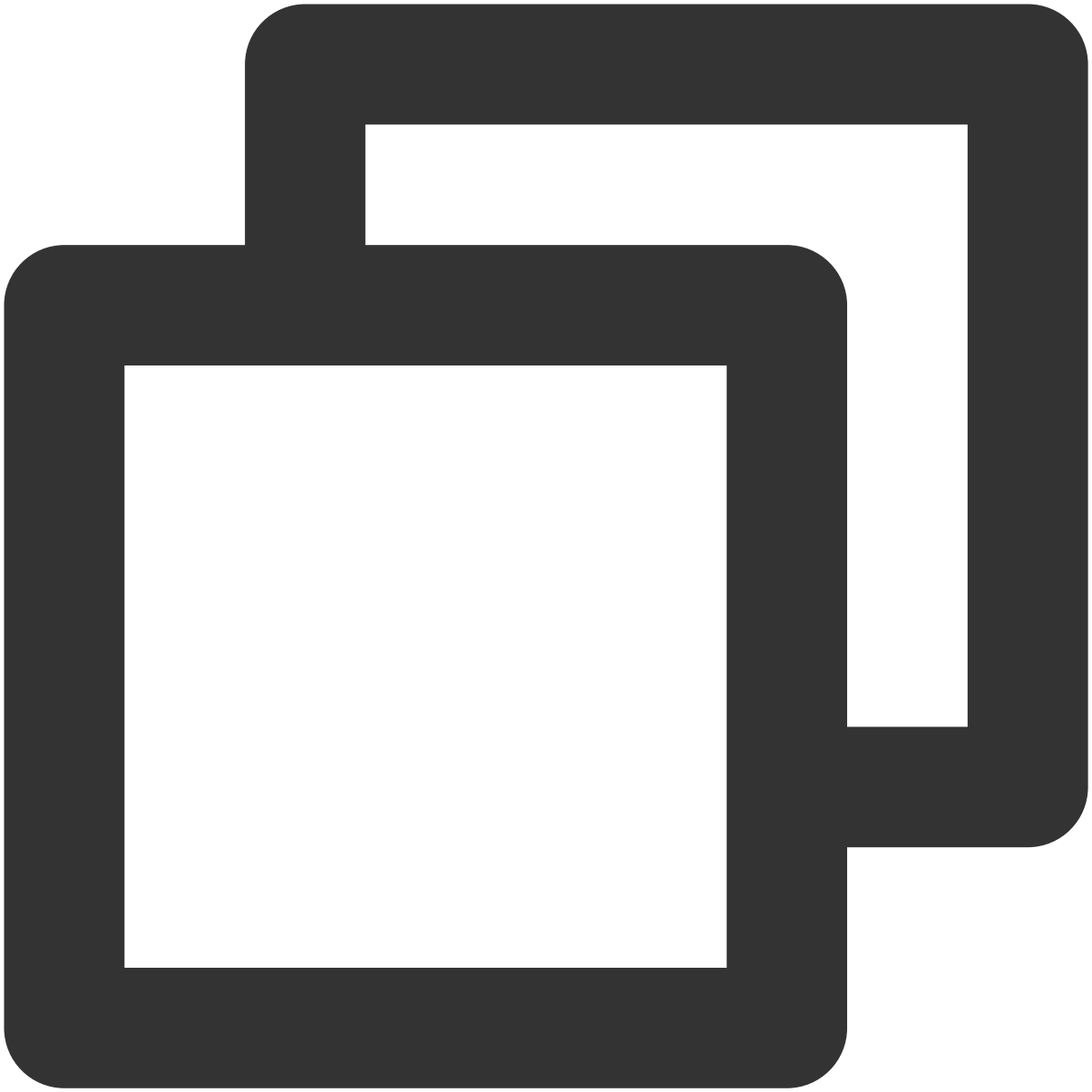
```
HTTP/1.1 400 Bad Request
WWW-Authenticate: Bearer error="invalid_request", error_description="Bearer token n
```

`bearer_token` 错误。



```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="invalid_token", error_description="Error decoding J
```

`bearer_token` 无效。



```
HTTP/1.1 403 Forbidden
WWW-Authenticate: Bearer error="insufficient_scope", error_description="The request
```

重置用户密码

最近更新时间：2023-12-22 11:42:07

接口描述

重置用户的密码。调用此接口前，需要先通过 发送_OTP_验证码 接口向用户发送验证码。

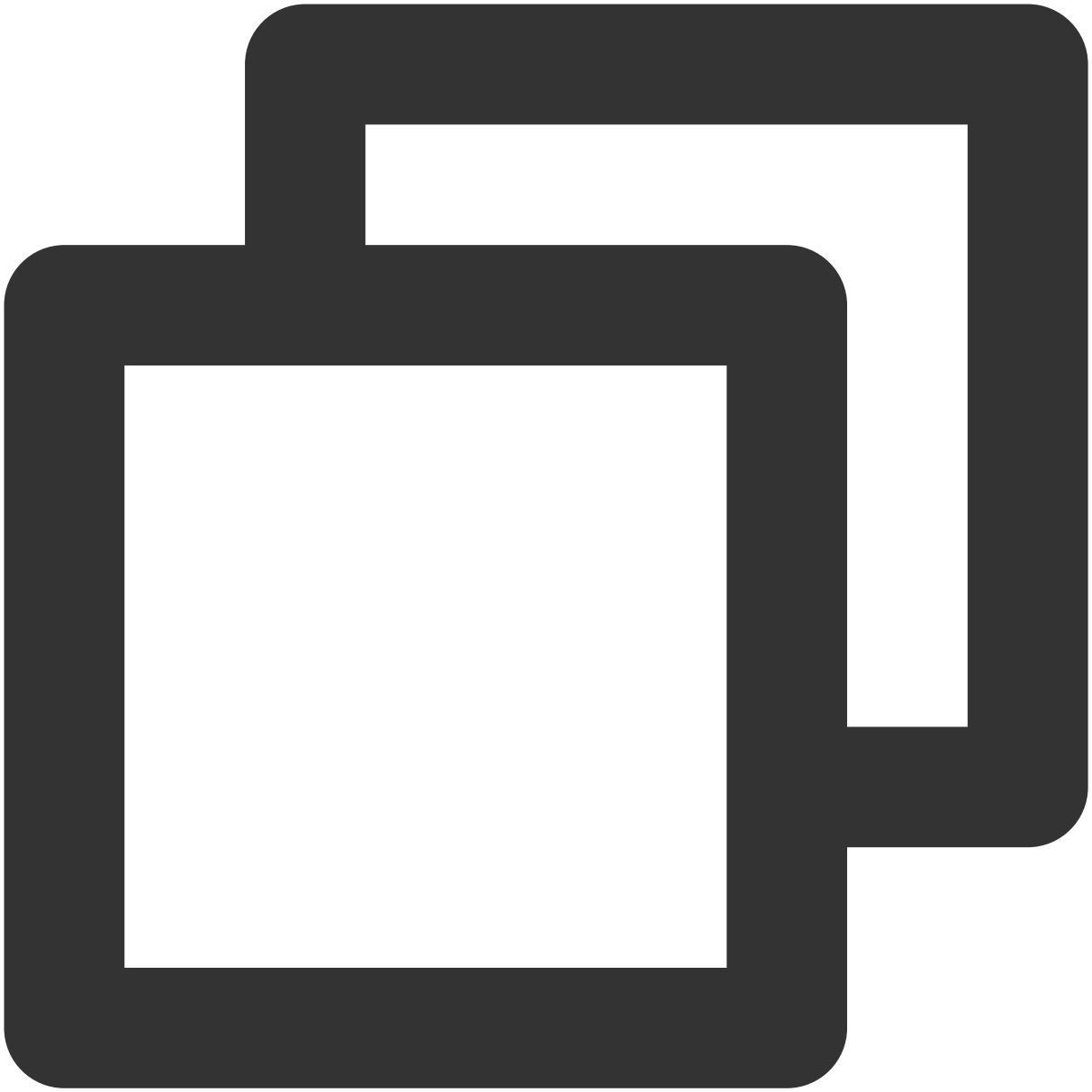
注意：

新密码需符合当前应用关联的账号密码认证源的密码策略，且不能与策略中指定的前 N 次历史密码相同。

支持的应用类型

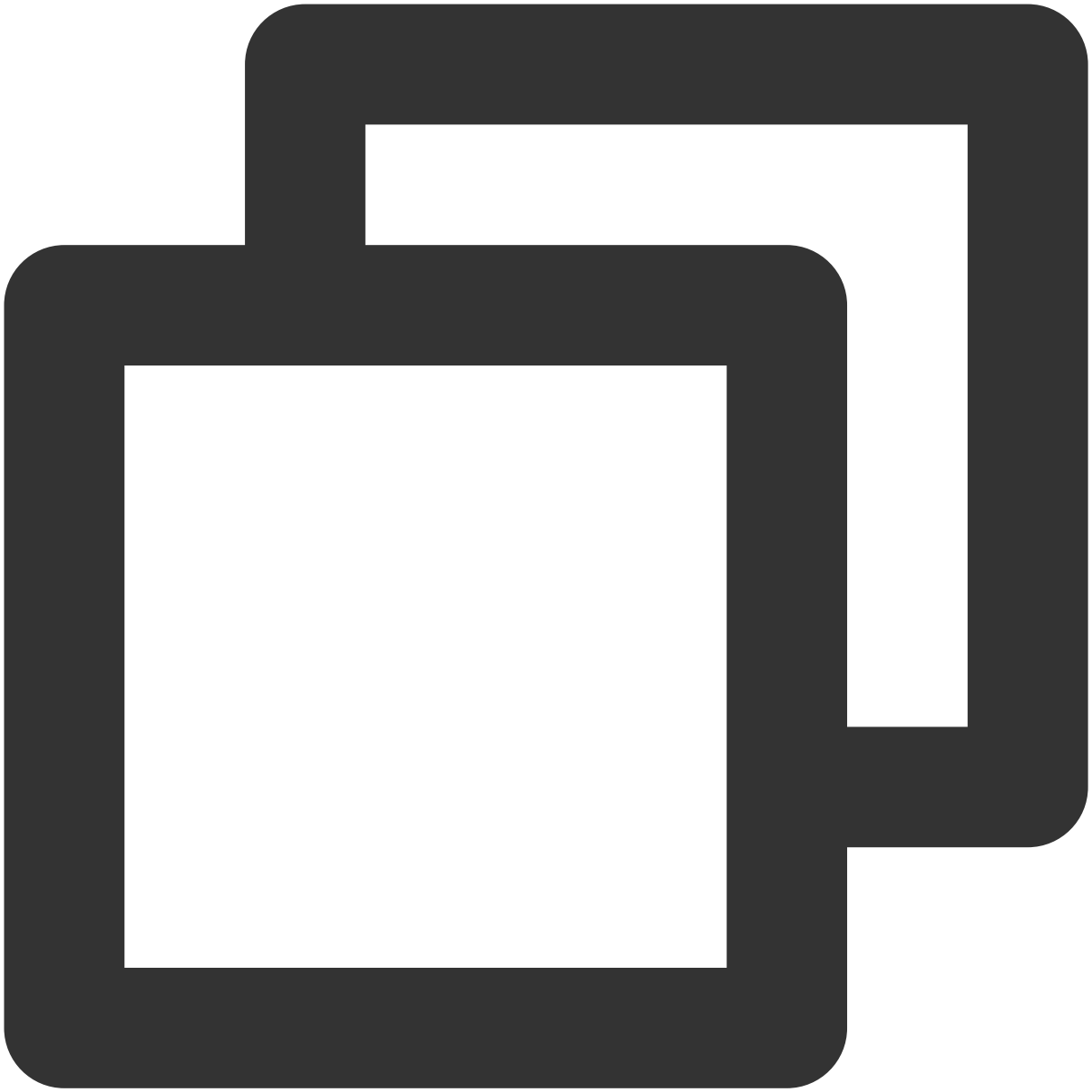
Web 应用、单页应用、移动 App。

请求方法



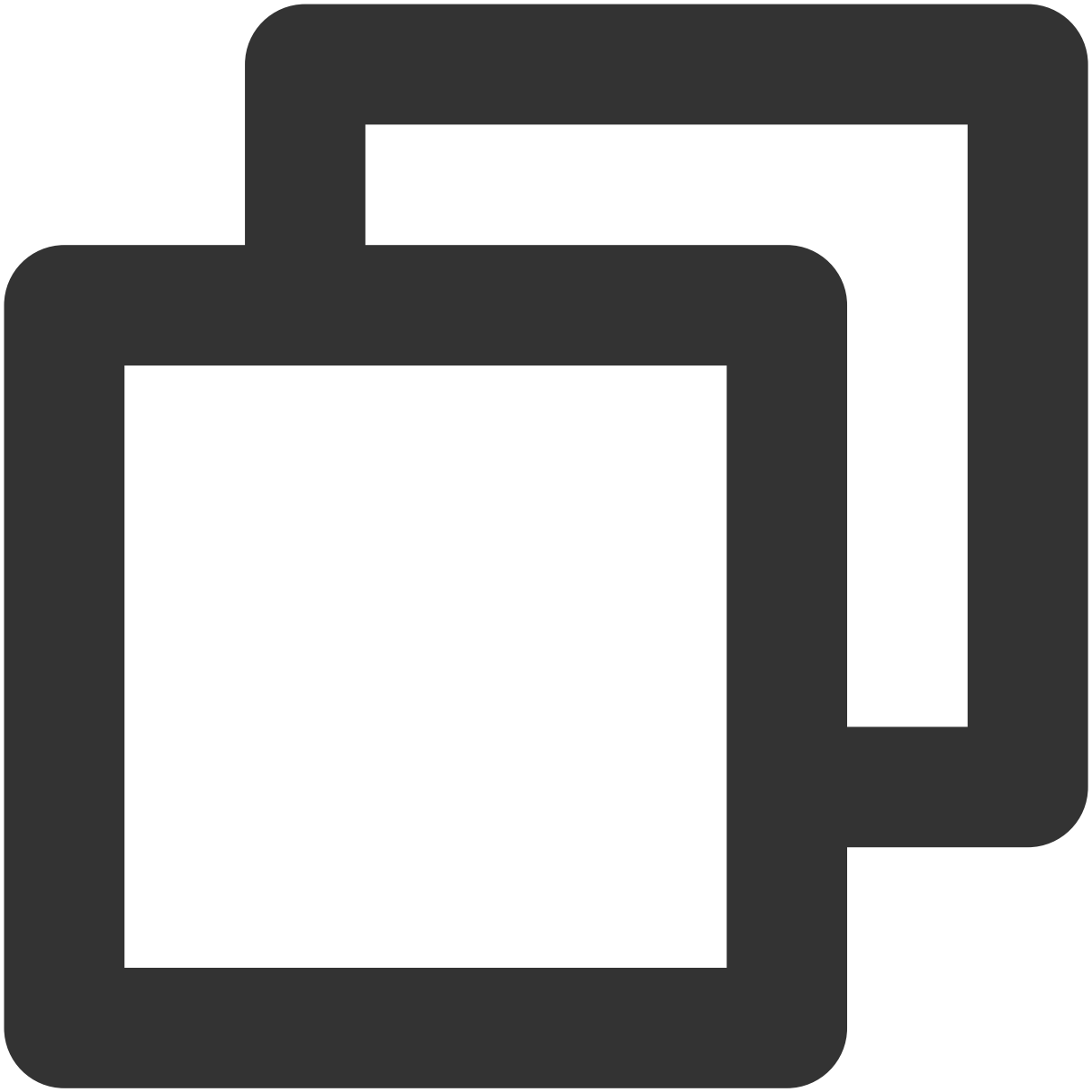
```
POST
```

请求路径



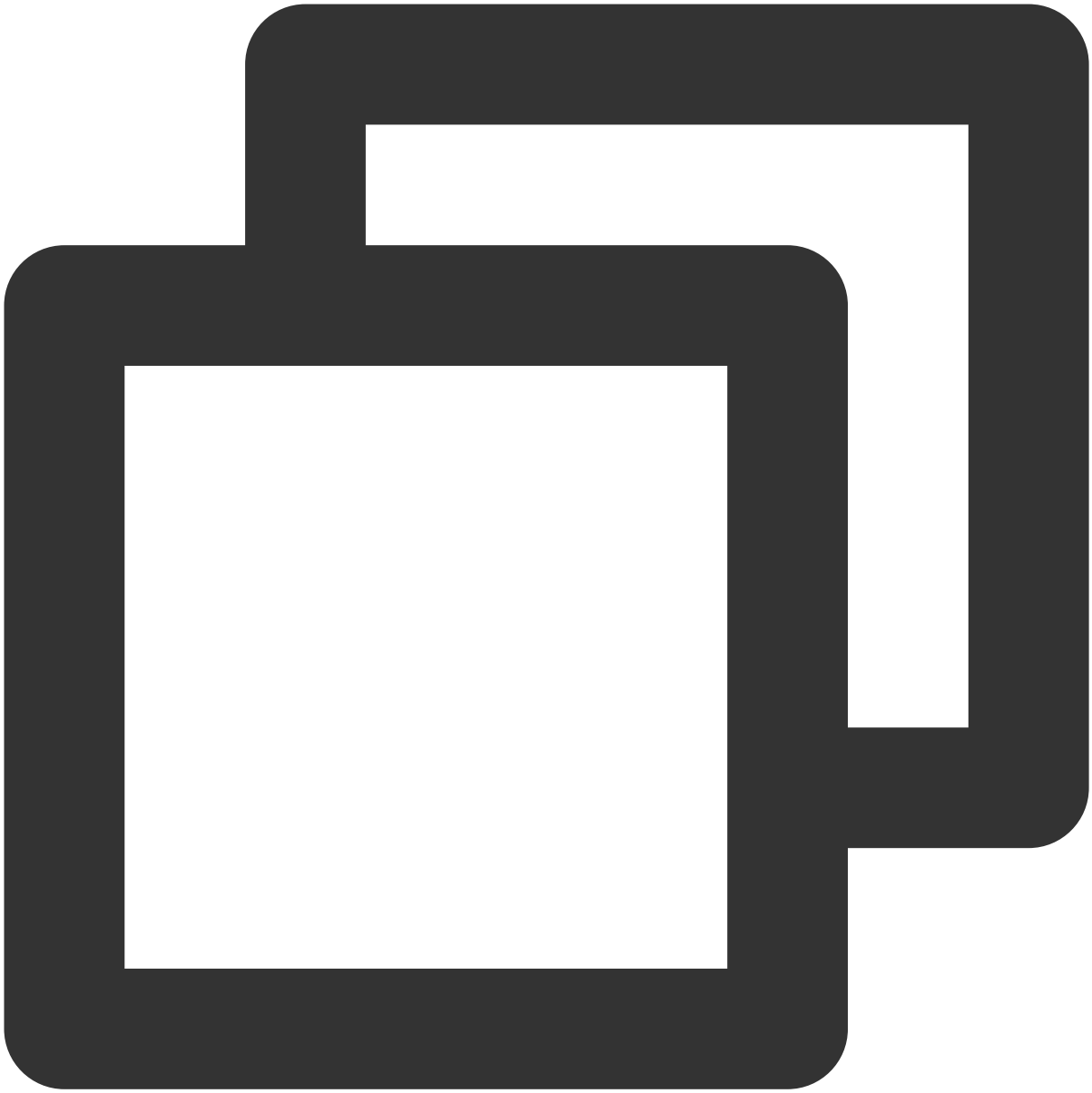
```
/reset_user_password
```

请求 Content-Type



```
application/json
```

请求示例



```
POST /reset_user_password HTTP/1.1
Content-Type: application/json
Authorization: Basic VEVOQU5UX0NMSUVOVF9JRDpURU5BTlRfQ0xJRU5UX1NFQ1JFVA==
Host: sample.portal.tencentciam.com

{
    "password" : "MOCK_PASSWORD",
    "email" : "MOCK_EMAIL@163.com",
    "email_otp" : "MOCK_EMAIL_OTP",
    "email_otp_token" : "MOCK_EMAIL_OTP_TOKEN"
}
```

请求头

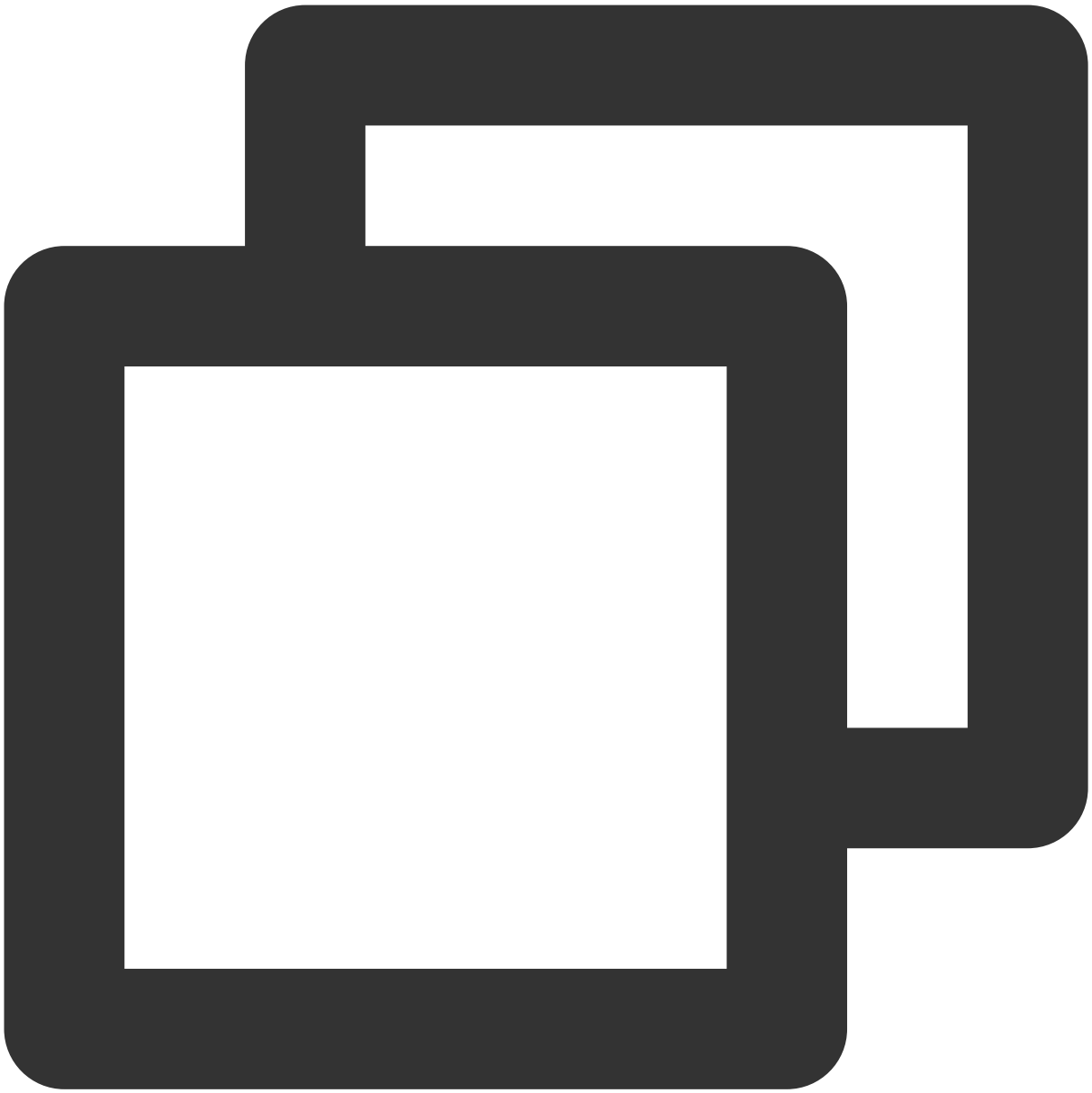
名称	描述
Authorization	HTTP Basic 认证请求头，格式为 `Basic <credentials>` ，其中 Basic 为固定字符串， `<credentials>` 的计算方式为 `base64(url_encode(client_id) + ":" + url_encode(client_secret))` ，Basic 和 `<credentials>` 之间用一个空格隔开。

请求体 JSON 参数

JSON 路径	数据类型	描述
client_id	String	应用的 client_id。需要与发送验证码时使用的一致。
client_secret	String	应用的 client_secret。Web 应用须传递此参数。单页应用和移动 App 不传递此参数。
password	String	新密码。
email	String	用户的邮箱地址。发送邮箱 OTP 验证码时传递此参数。
email_otp_token	String	发送邮箱验证码成功后服务端返回的 otp_token。
email_otp	String	用户邮箱收到的 OTP 验证码。
phone_number	String	用户的手机号。发送短信 OTP 验证码时传递此参数。
phone_number_otp_token	String	发送短信验证码成功后服务端返回的 otp_token。
phone_number_otp	String	用户手机收到的 OTP 验证码。

正常响应示例

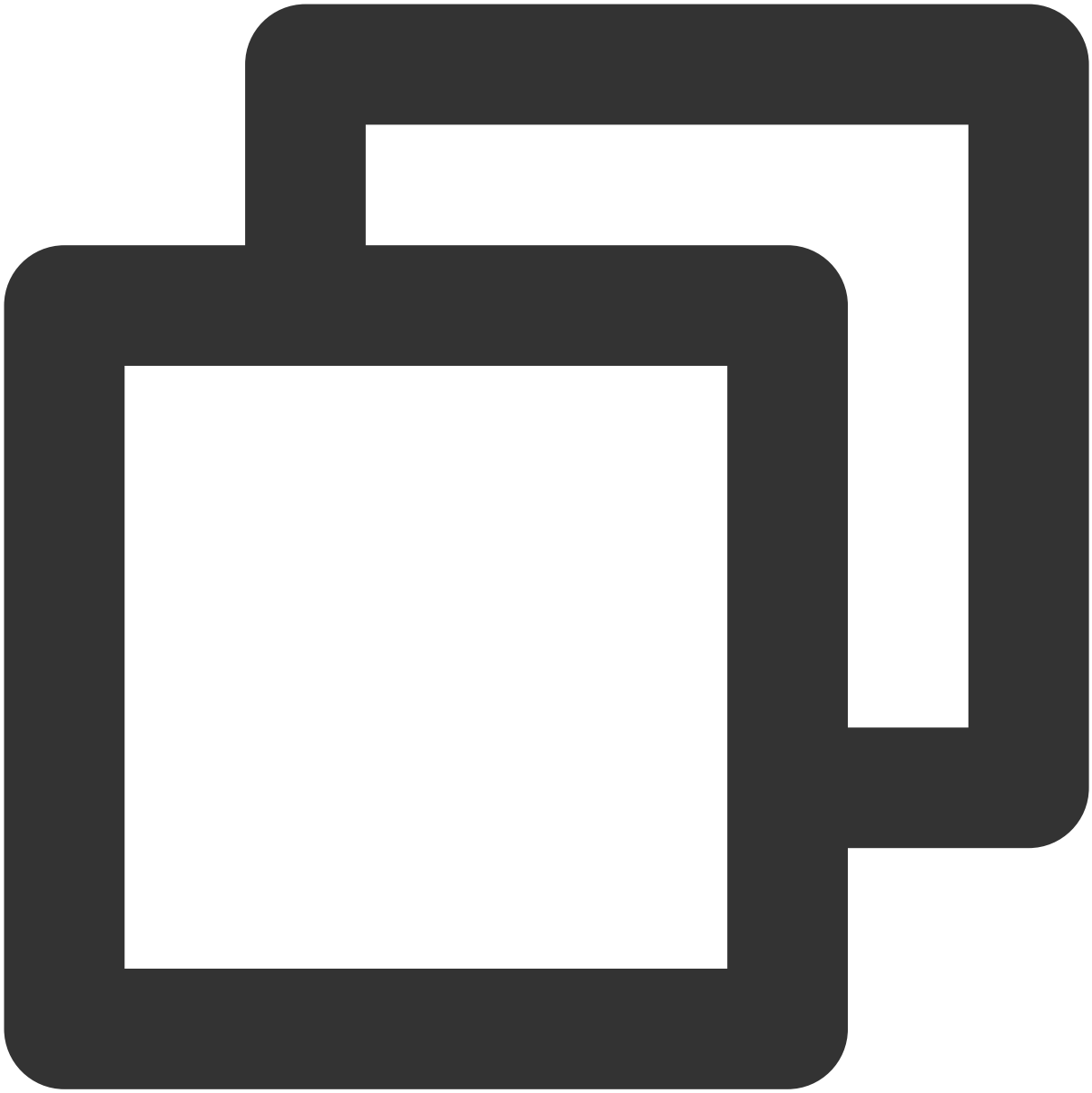
重置密码成功。



```
HTTP/1.1 200 OK
```

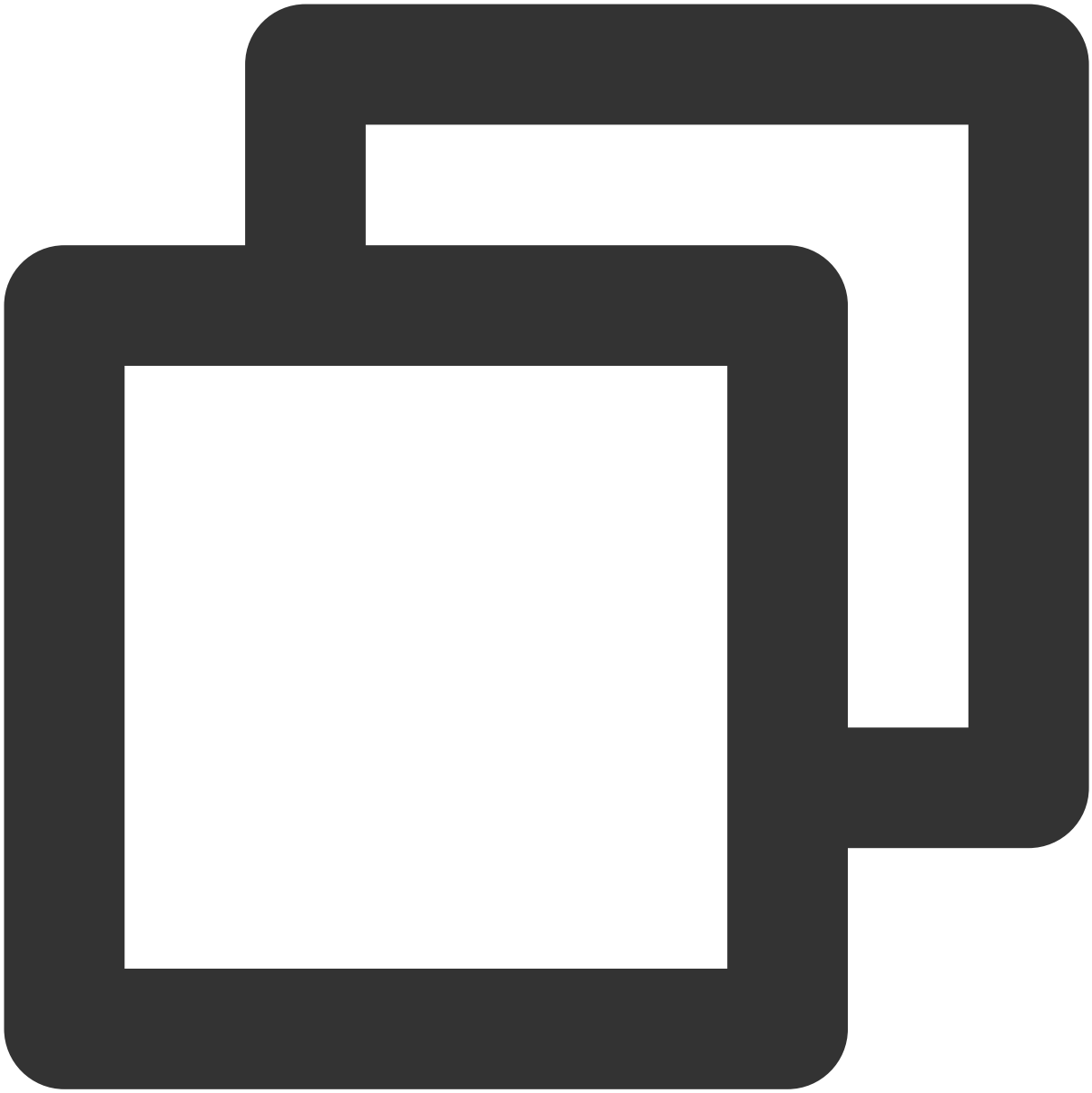
异常响应示例

新密码与历史密码相同。



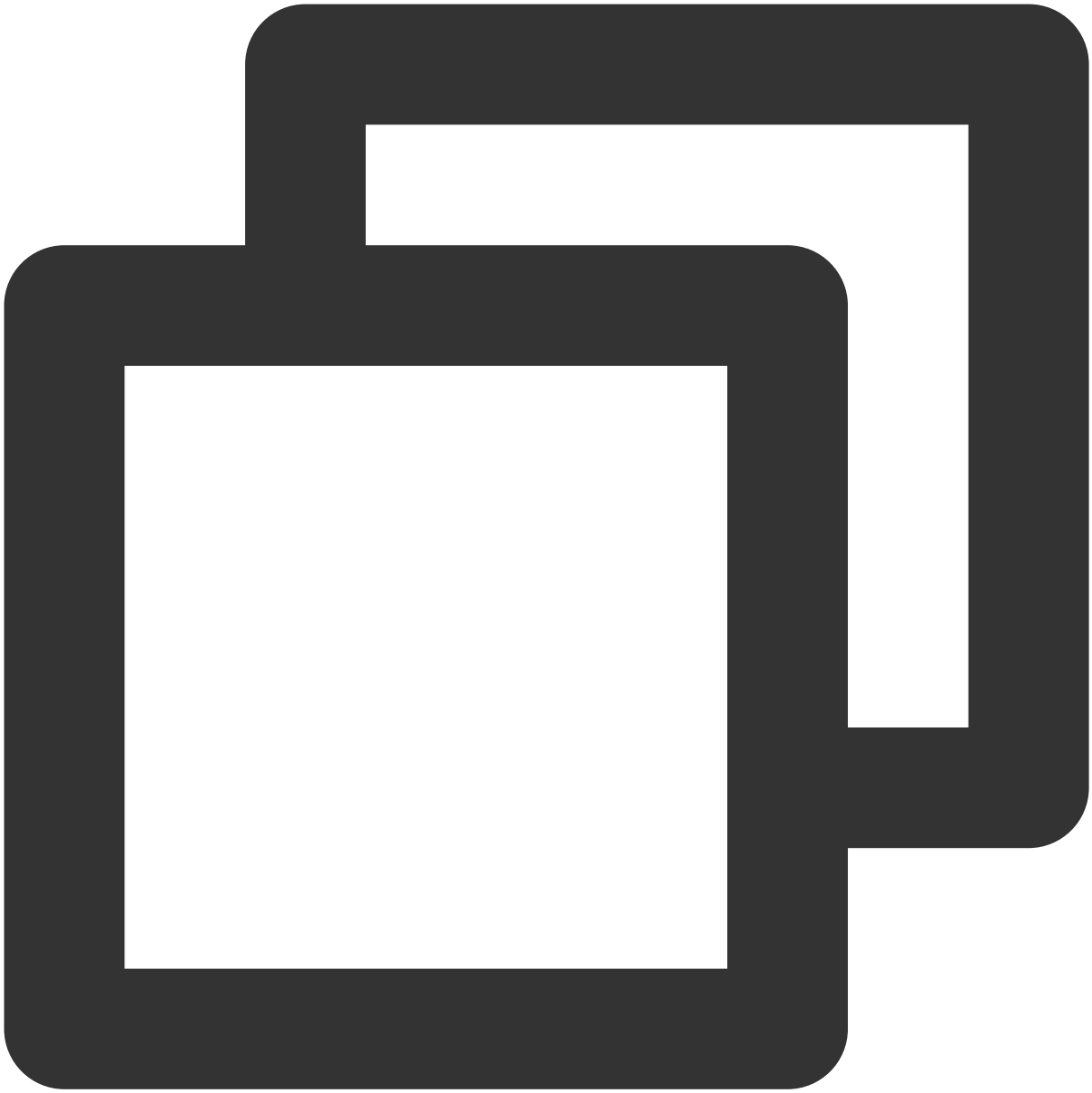
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "recurrent_password"
}
```

新密码不满足密码策略。



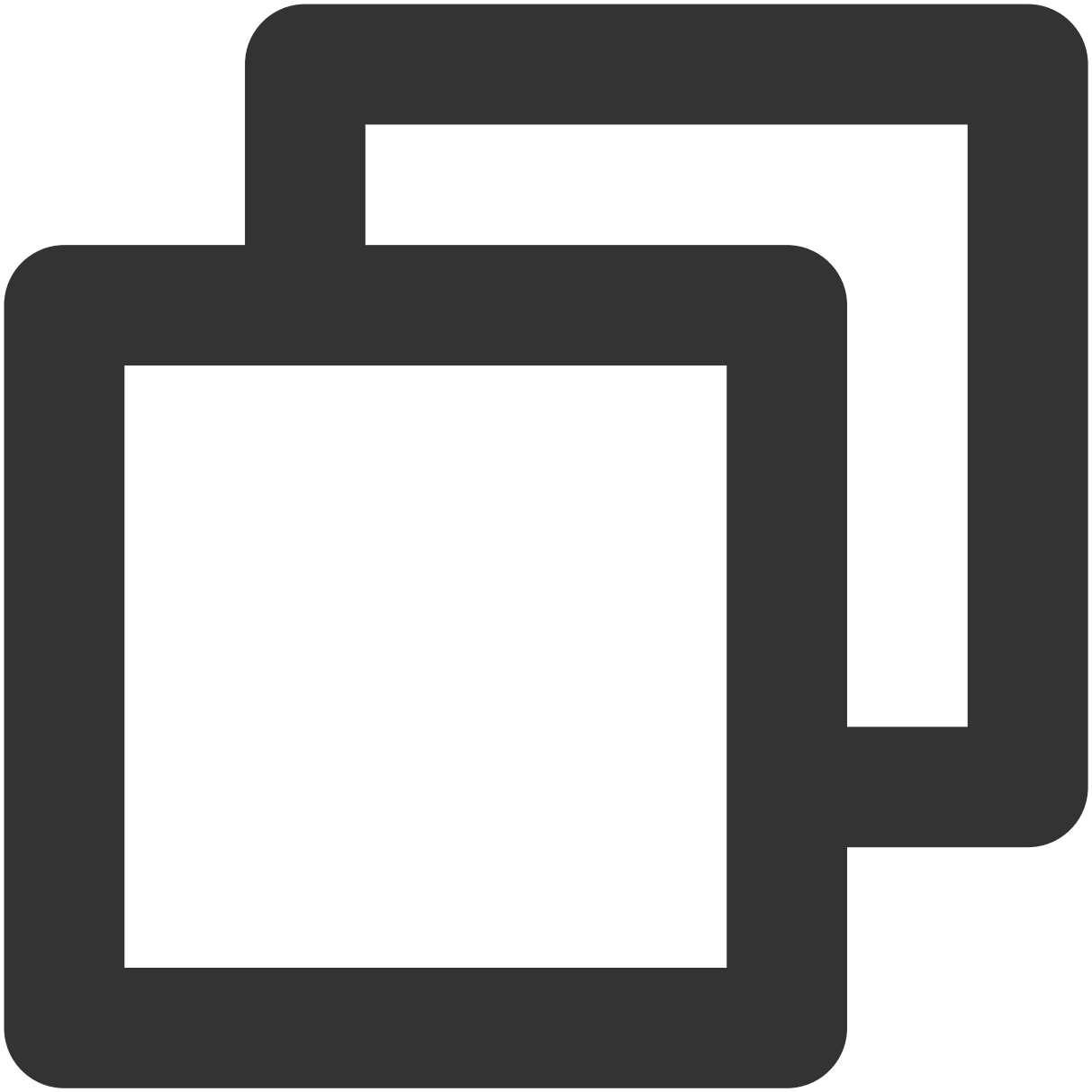
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_new_password"
}
```

未找到与 email 对应的用户。



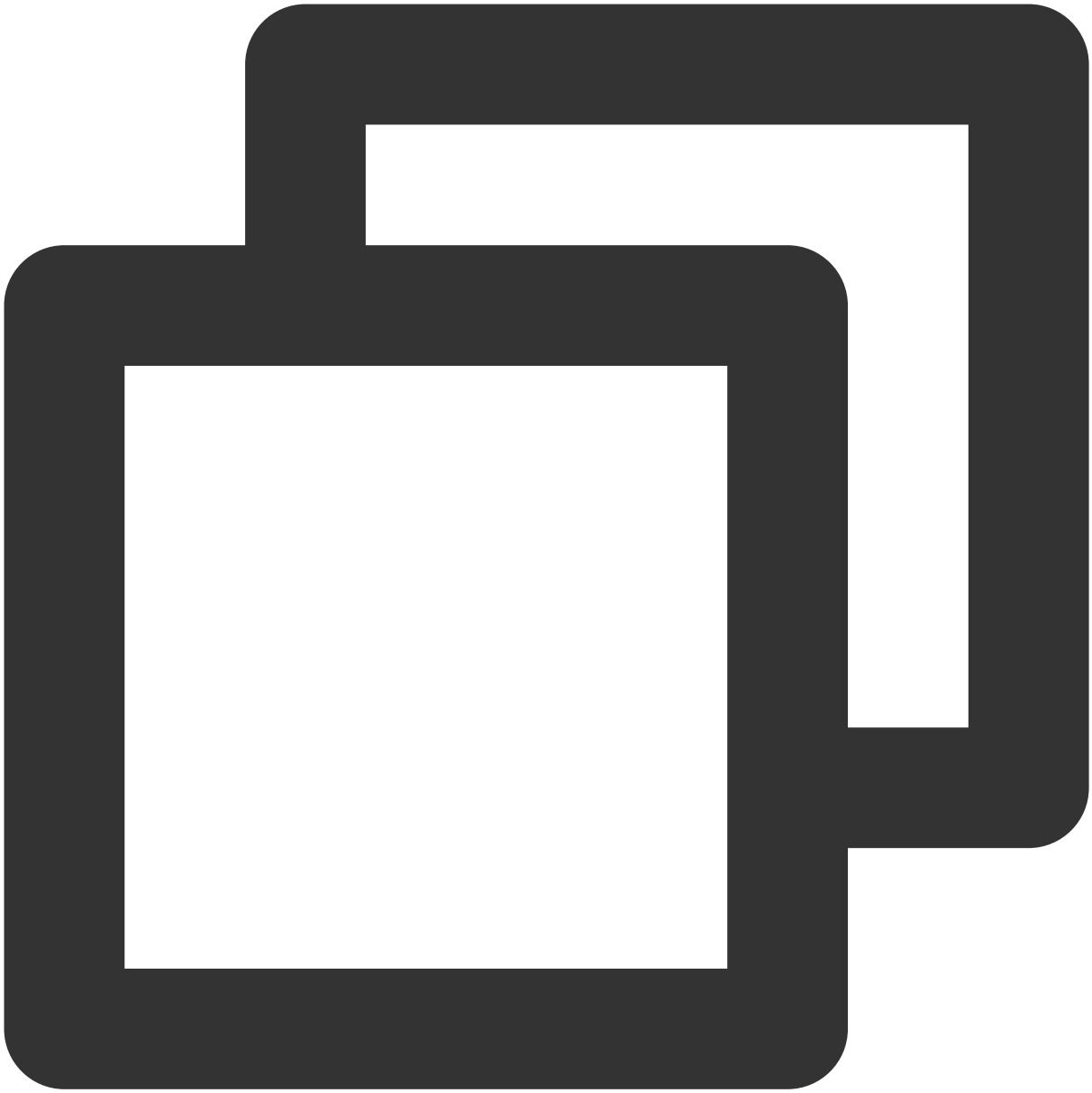
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "user_not_found"
}
```

用户处于冻结状态，无法重置密码。



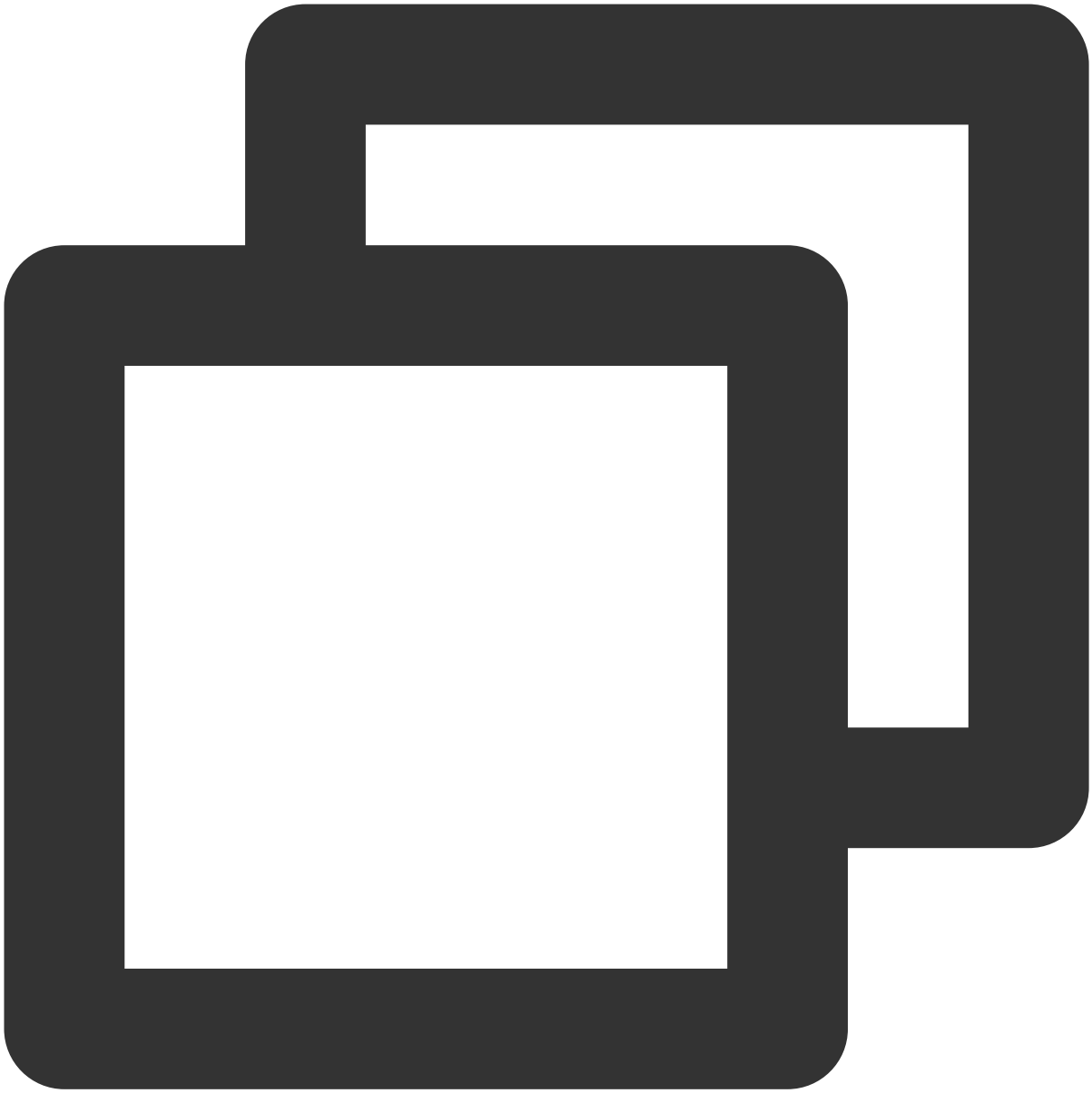
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "abnormal_user_status",
"error_description" : "User is frozen."
}
```

email_otp_token 错误或已过期，或重置密码时使用的参数与发送验证码时不一致（例如：邮箱不同）。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp_token"
}
```

email_otp 错误或已过期。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "bad_email_otp"
}
```

获取 Token
PKCE 授权码模式

最近更新时间：2023-12-22 11:42:08

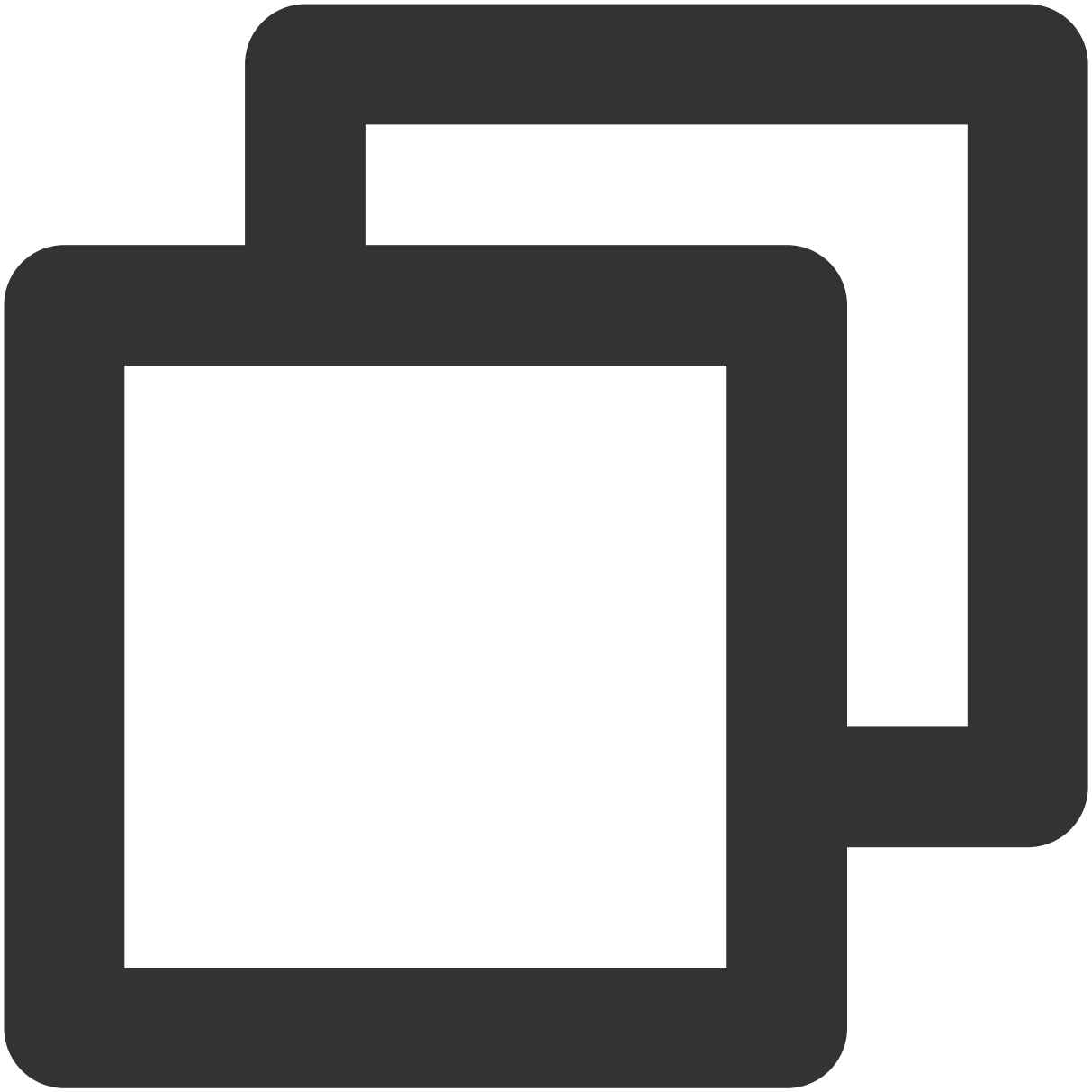
接口描述

应用系统通过 PKCE 授权码模式获得认证门户返回的 `code` 之后，调用此接口获取 Access Token 和 ID Token，完成登录。

支持的应用类型

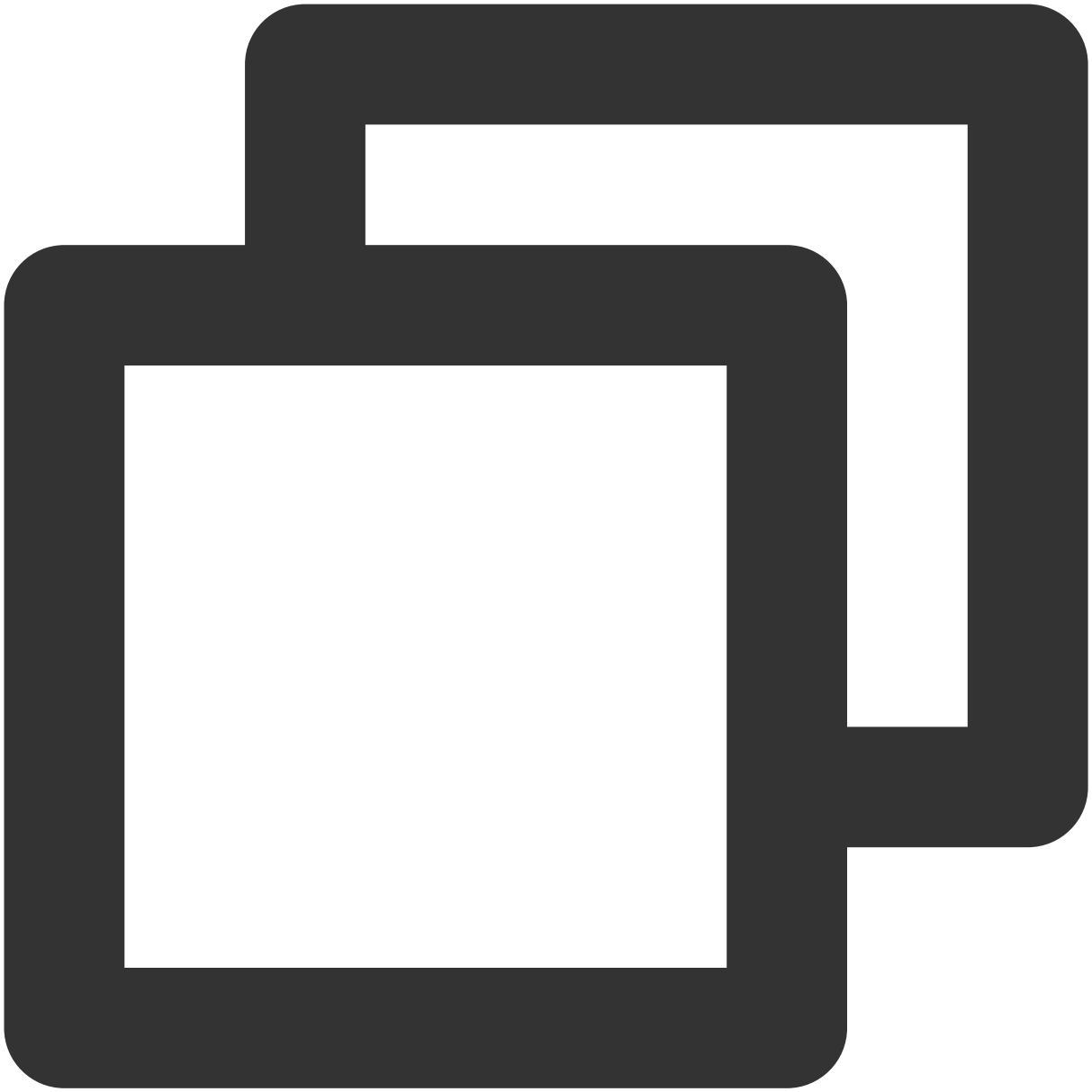
Web 应用、单页应用、移动 App。

请求方法



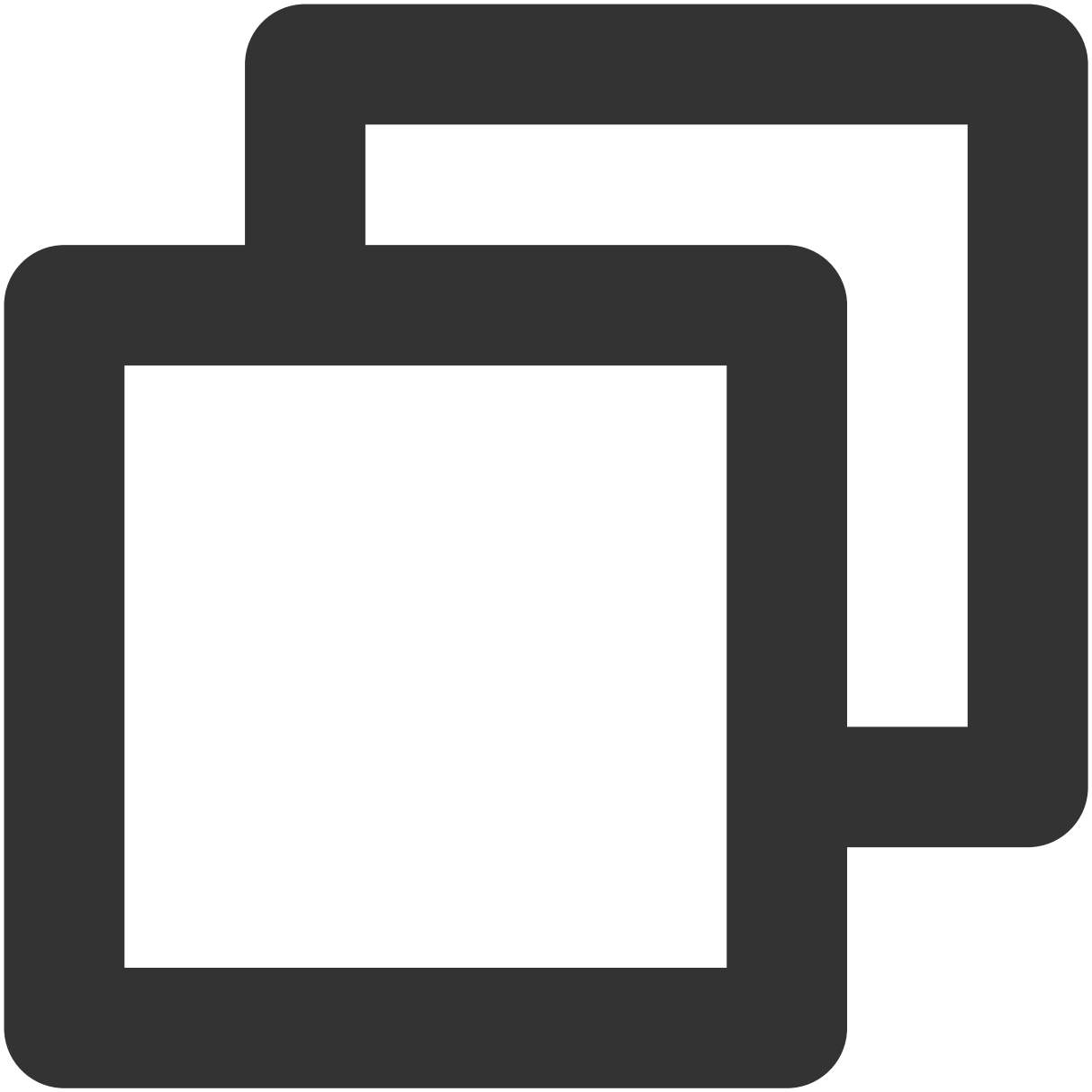
```
POST
```

请求路径



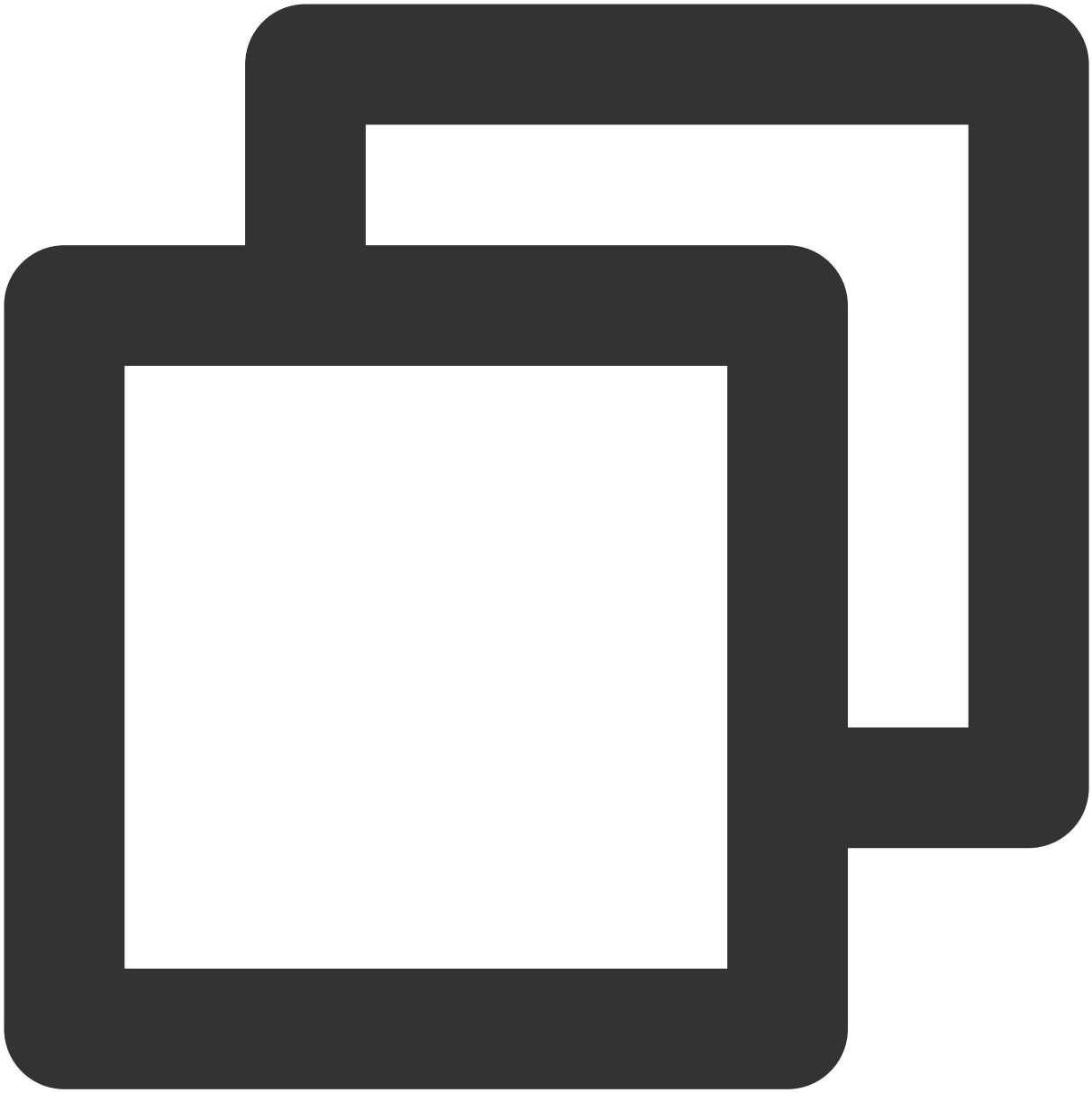
```
/oauth2/token
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例

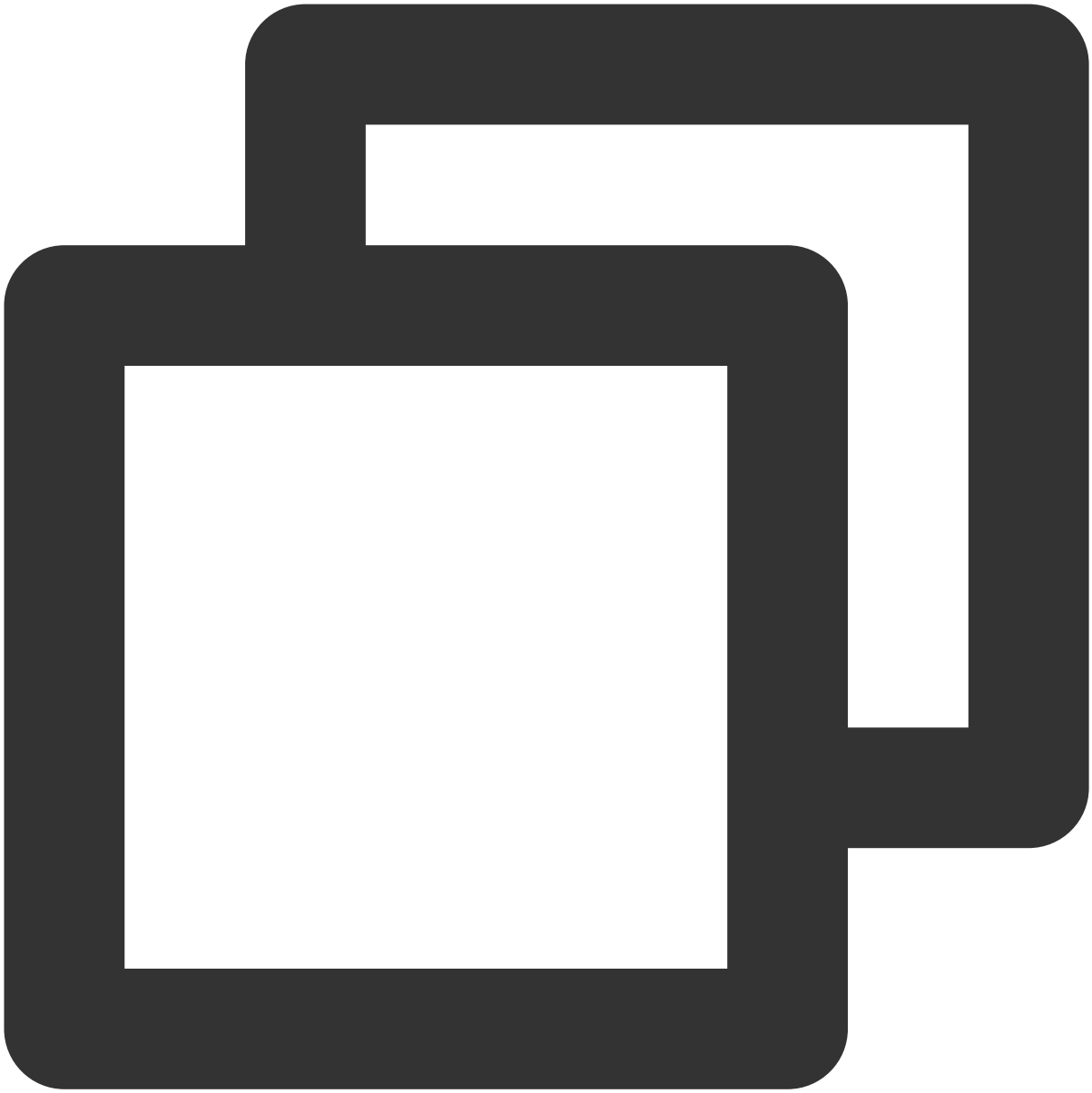


```
POST /oauth2/token HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded

client_id=TENANT_CLIENT_ID&grant_type=authorization_code&code=MOCK_CODE&redirect_ur
```

请求参数

参数	可选	描述
client_id	false	应用的 `client_id` 。需要与获取授权时使用的一致。
grant_type	false	填固定值 `authorization_code` 。
code	false	获取授权时返回的授权码。
redirect_uri	false	授权成功后的重定向地址。需要与获取授权时指定的地址一致。
code_verifier	false	PKCE code_verifier 。需要与获取授权时用于生成 code_challenge 的 code_verifier 一致。

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ
  "refresh_token" : "8FuXWpwMZI9oA8ASvCUrqap61N7RvPON6DjWFk-Saiv4dOR8y2tNf9eKf36woA
  "scope" : "openid",
  "id_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ0eXA
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

响应参数

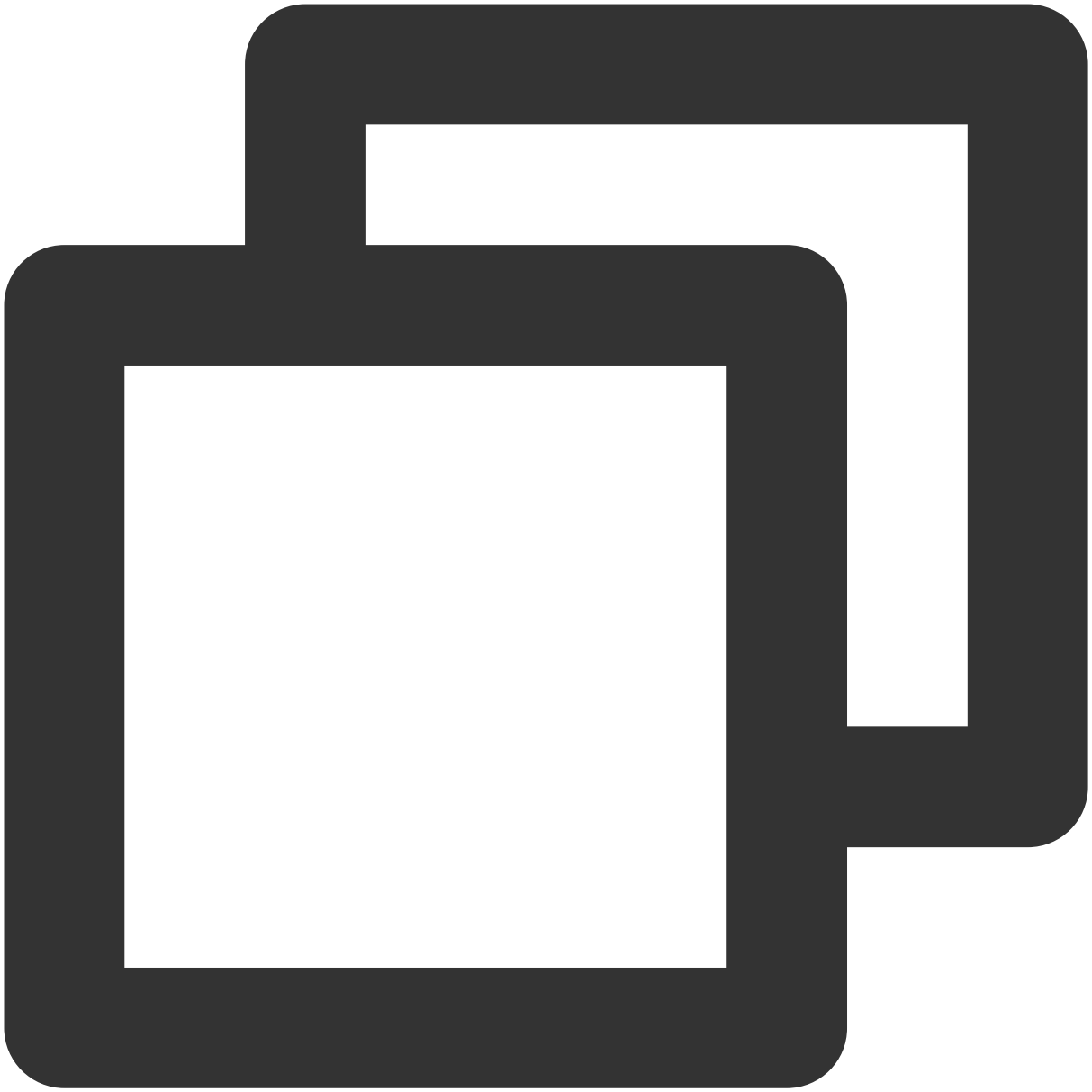
参数	数据类型	描述
access_token	String	OAuth 2.0 Access Token (JWT)。
refresh_token	String	OAuth 2.0 Refresh Token。
scope	String	Access Token 的 Scope。
id_token	String	OIDC ID Token (JWT)。
token_type	String	Token 类型，目前取固定值 `Bearer` 。
expires_in	Number	Access Token 有效期，单位秒。

说明：

CIAM 返回的是 JWT 格式的 ID Token，请参考 OIDC 官方文档 对 ID Token 进行解密验证。也可以直接使用相关的开发库完成解密验证。 验证所需的公钥通过调用 获取 JWT 公钥 接口获得。

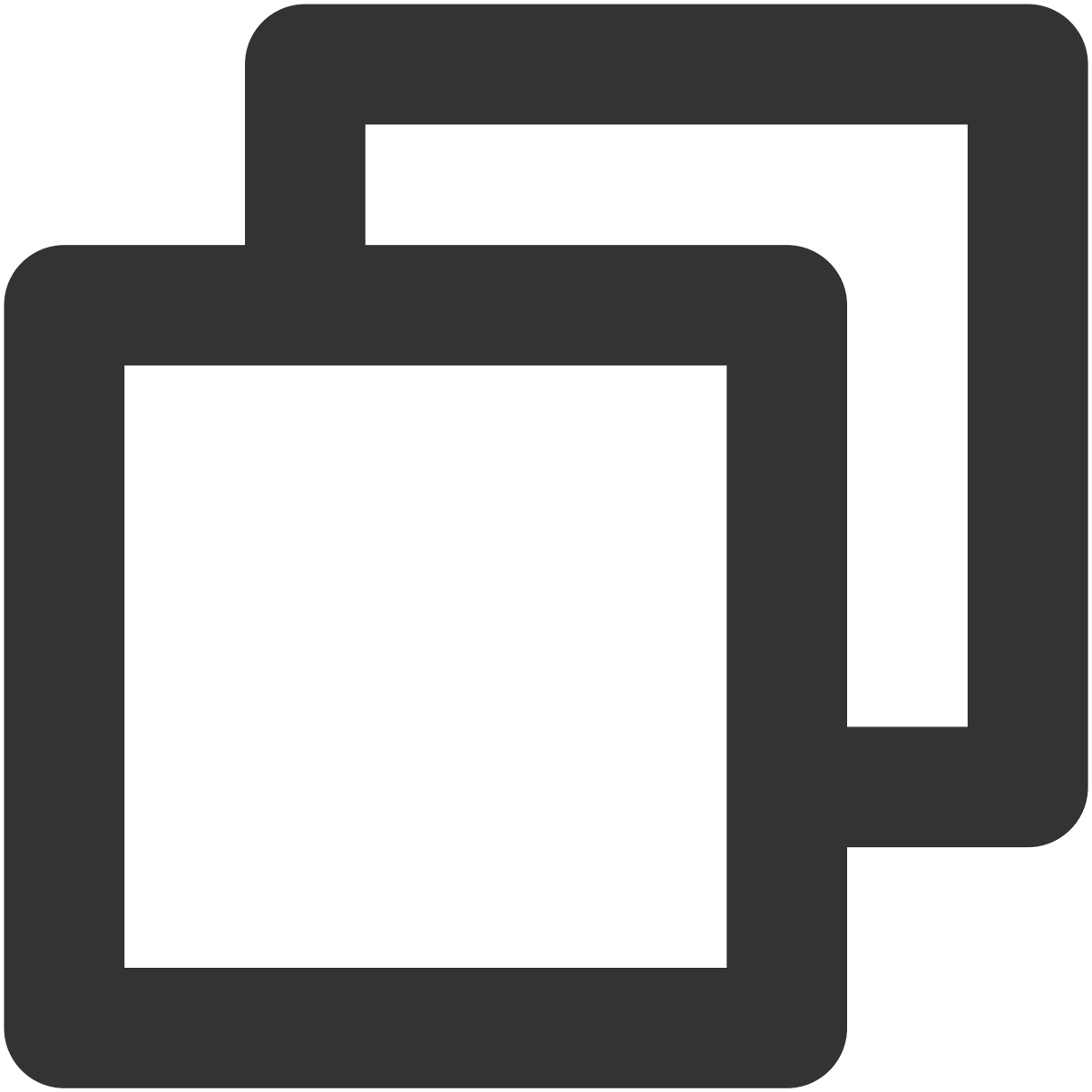
异常响应示例

client_id 参数缺失或有误。



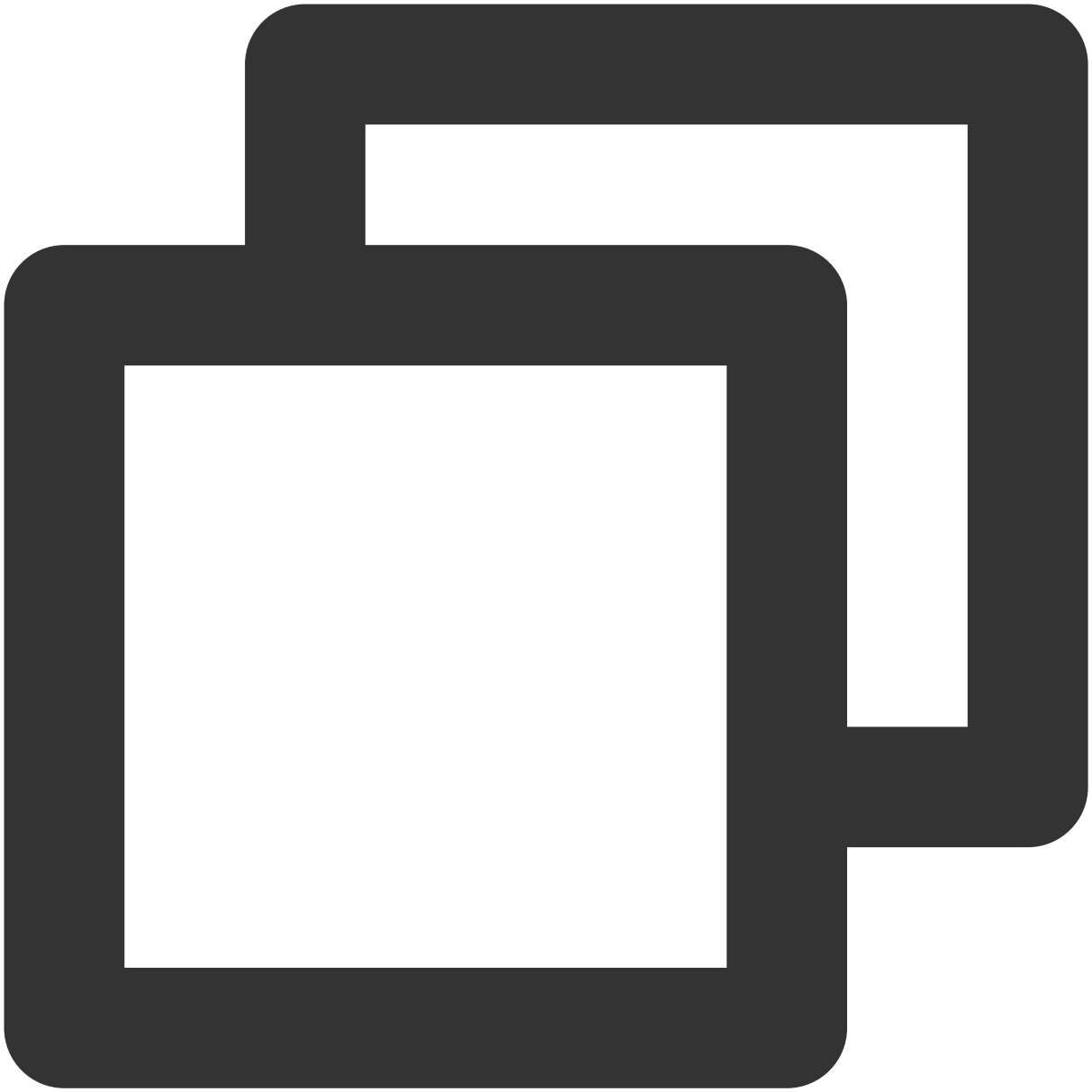
```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
{
"error" : "invalid_request"
}
```

client_id 与获取授权和获取 Token 时使用的不一致。



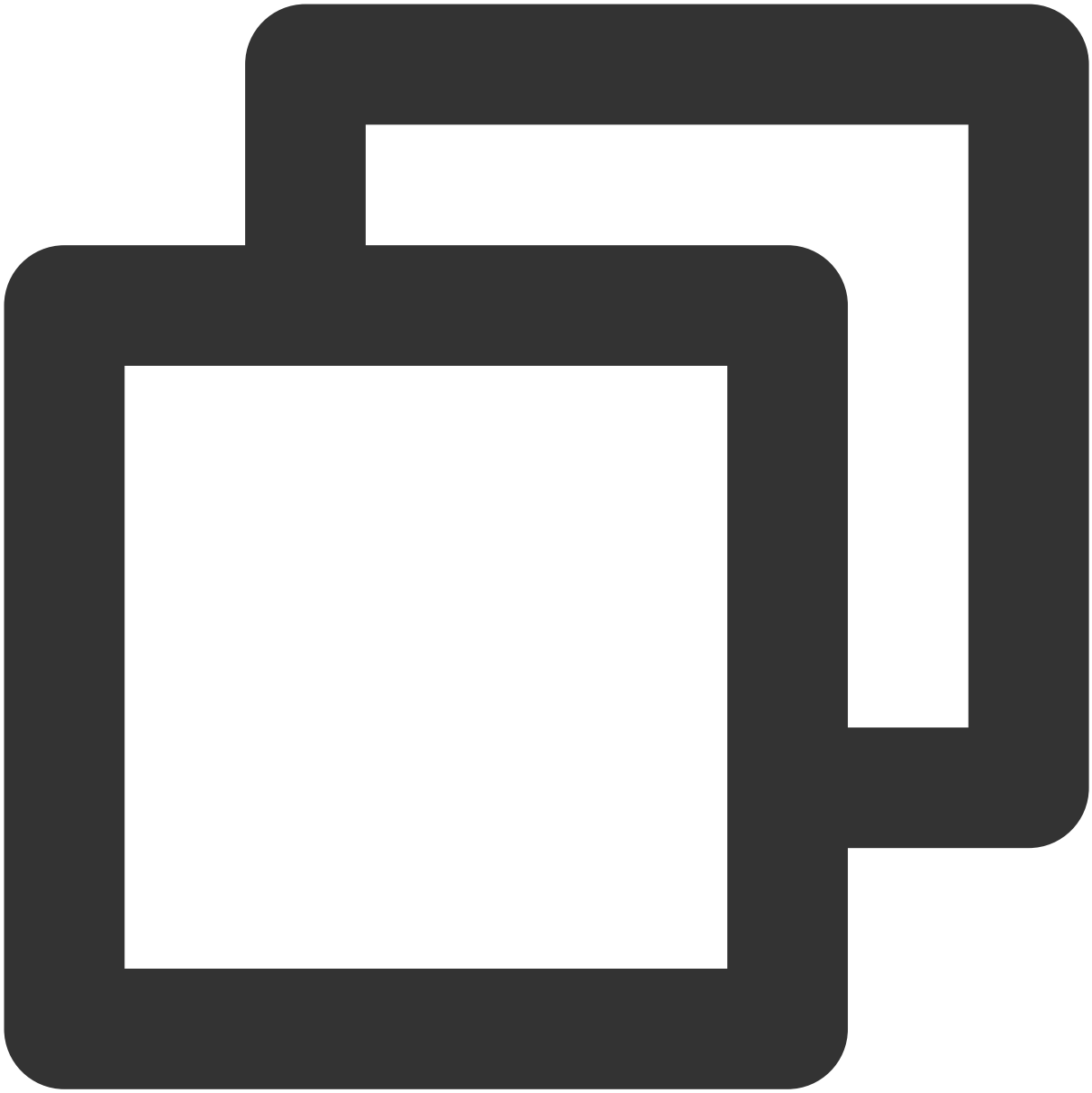
```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8
{
"error" : "invalid_client"
}
```

grant_type 参数有误。



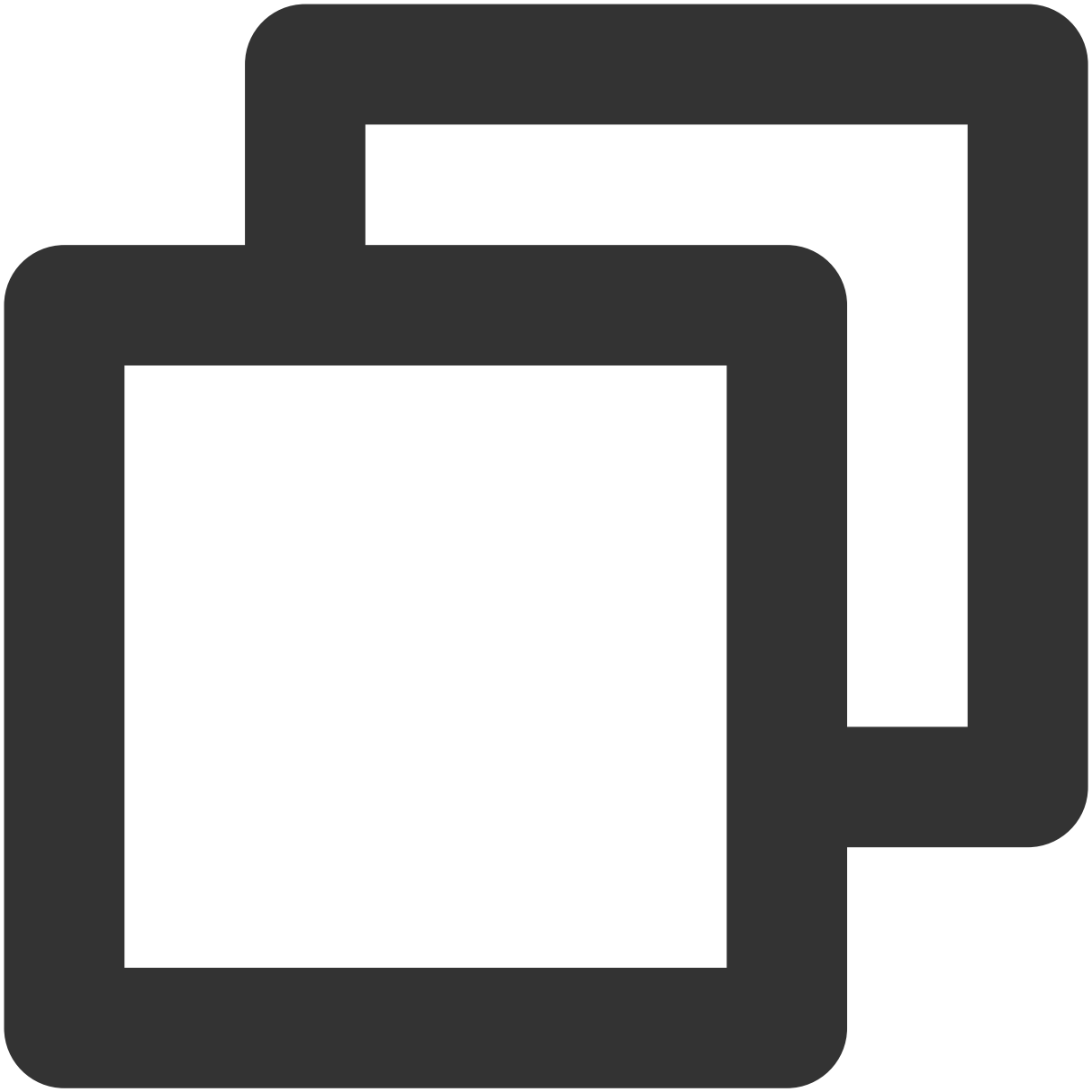
```
HTTP/1.1 401 Unauthorized
```

code 参数有误。



```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_client"
}
```

code_verifier 参数有误。



```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8
{
"error" : "invalid_client"
}
```

普通授权码模式

最近更新时间：2023-12-22 11:42:08

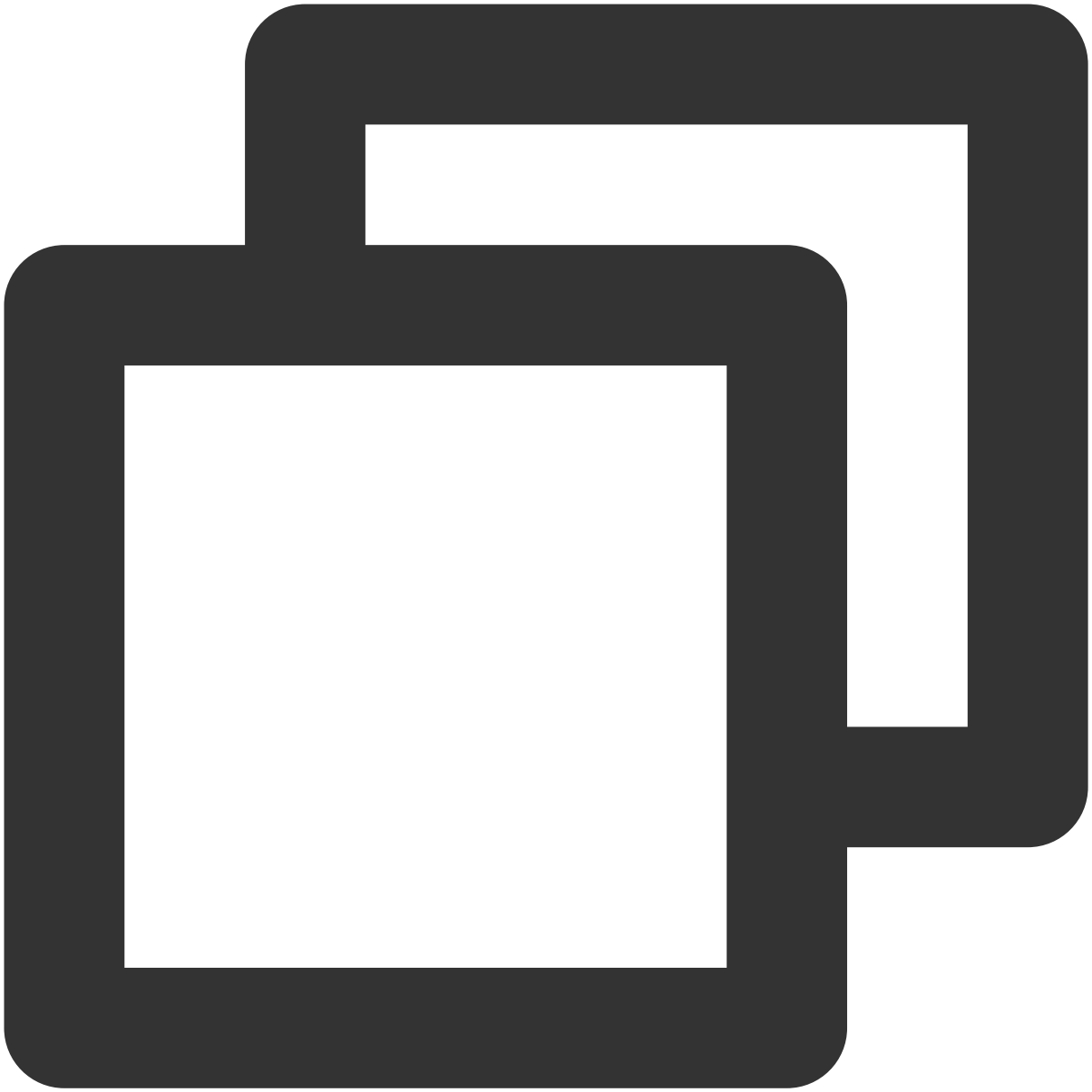
接口描述

应用系统通过普通授权码模式获得认证门户返回的 `code` 之后，调用此接口获取 Access Token 和 ID Token，完成登录。

支持的应用类型

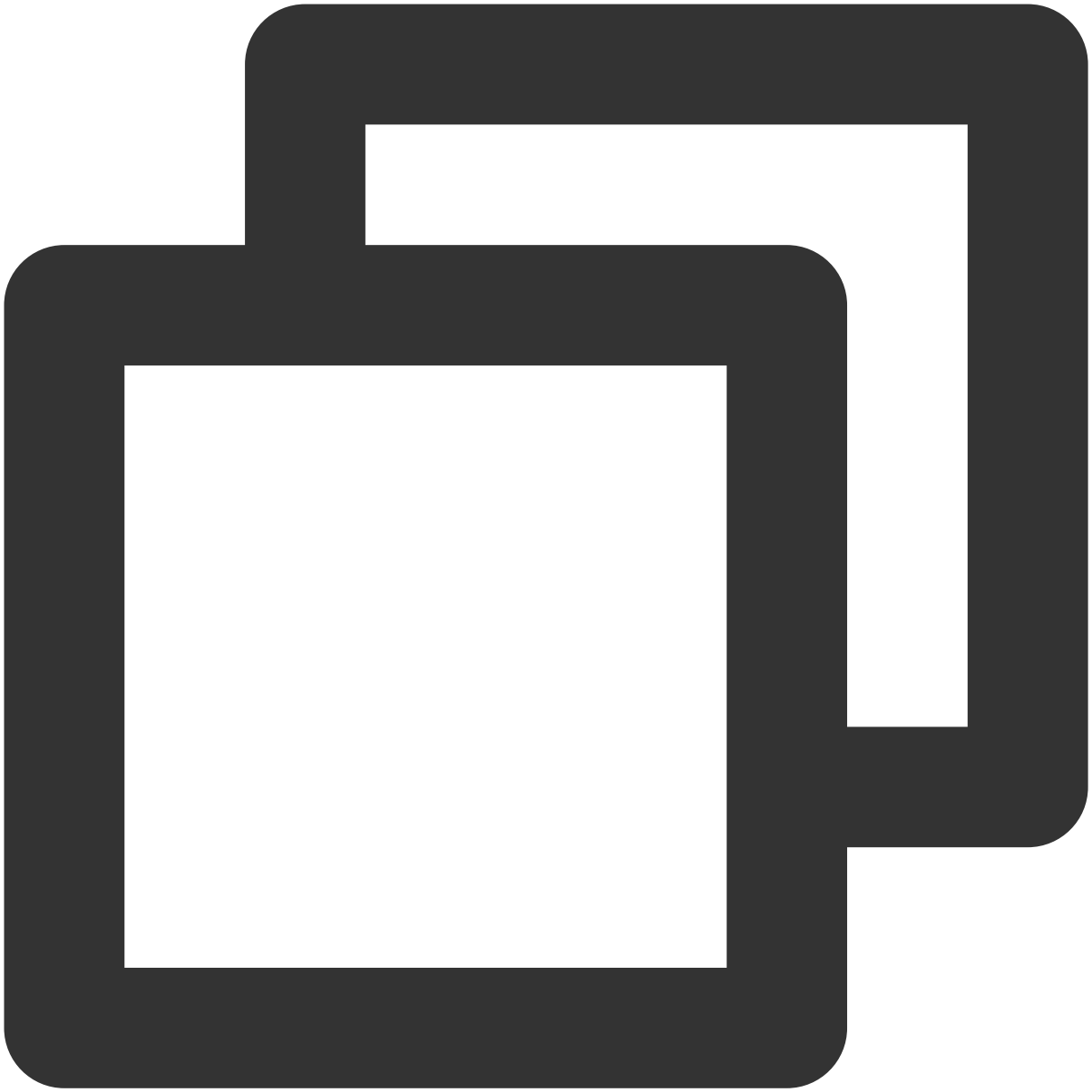
Web 应用、单页应用、移动 App。

请求方法



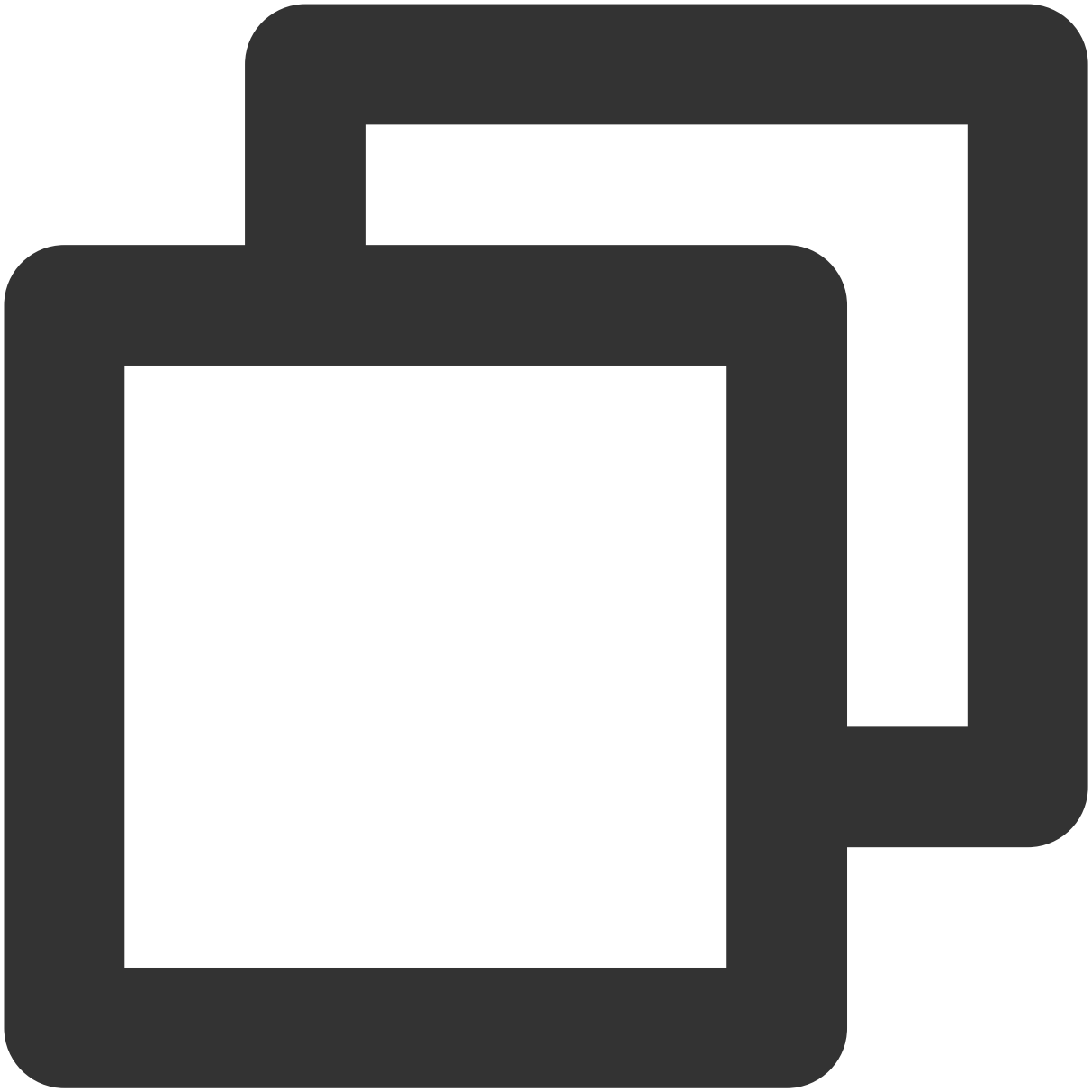
```
POST
```

请求路径



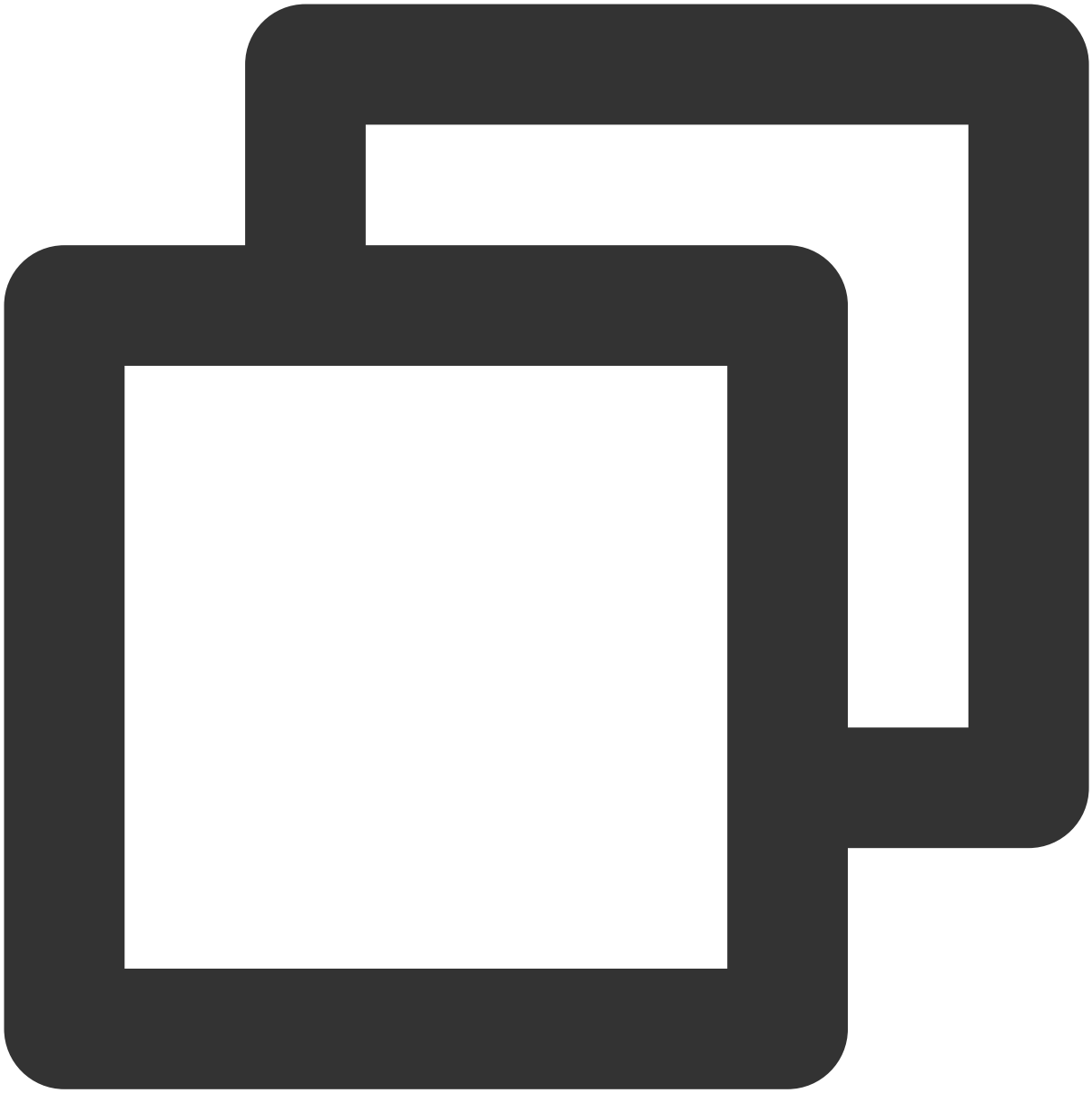
```
/oauth2/token
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例

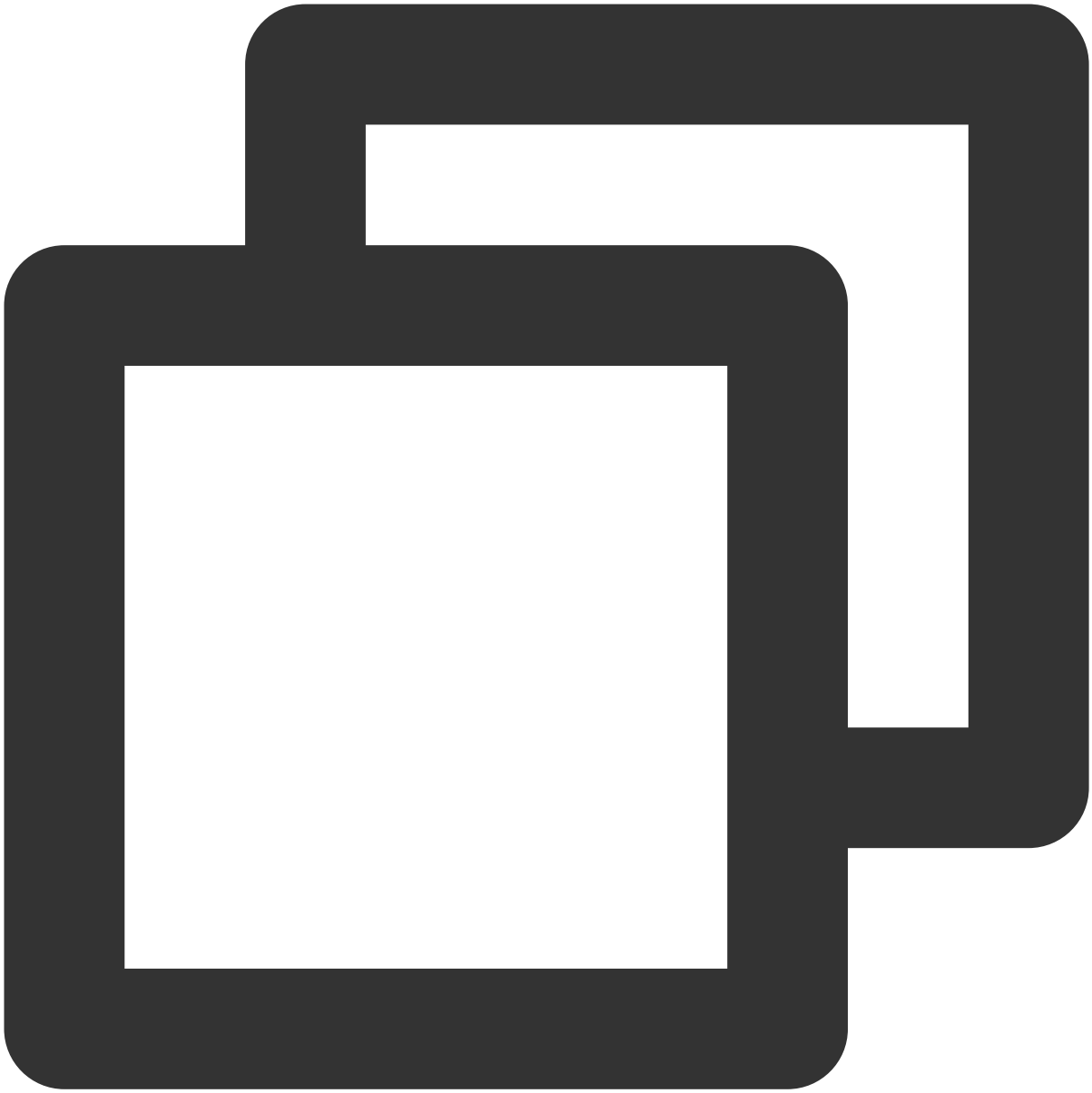


```
POST /oauth2/token HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded

client_id=TENANT_CLIENT_ID&client_secret=TENANT_CLIENT_SECRET&grant_type=authorizat
```

请求参数

参数	可选	描述
client_id	false	应用的 `client_id` 。需要与获取授权时使用的一致。
client_secret	false	应用的 `client_secret` 。可参考 **应用管理页面** > **选定指定应用** > 单击**应用配置** > 对应的“client_secret”。
grant_type	false	填固定值 `authorization_code` 。
code	false	获取授权时返回的授权码。
redirect_uri	false	授权成功后的重定向地址。需要与获取授权时指定的地址一致。

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ
  "refresh_token" : "Ugvo1lO7Se8vvIPrIOwn_eBe0hoi5-5ynR3H-aFYl0e1Gej-SfUAaBDBXkWmoj
  "scope" : "openid",
  "id_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ0eXA
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

说明：

CIAM 返回的是 JWT 格式的 ID Token，请参考 OIDC 官方文档 对 ID Token 进行解密验证。也可以直接使用相关的开发库完成解密验证。 验证所需的公钥通过调用 获取 JWT 公钥 接口获得。

响应参数

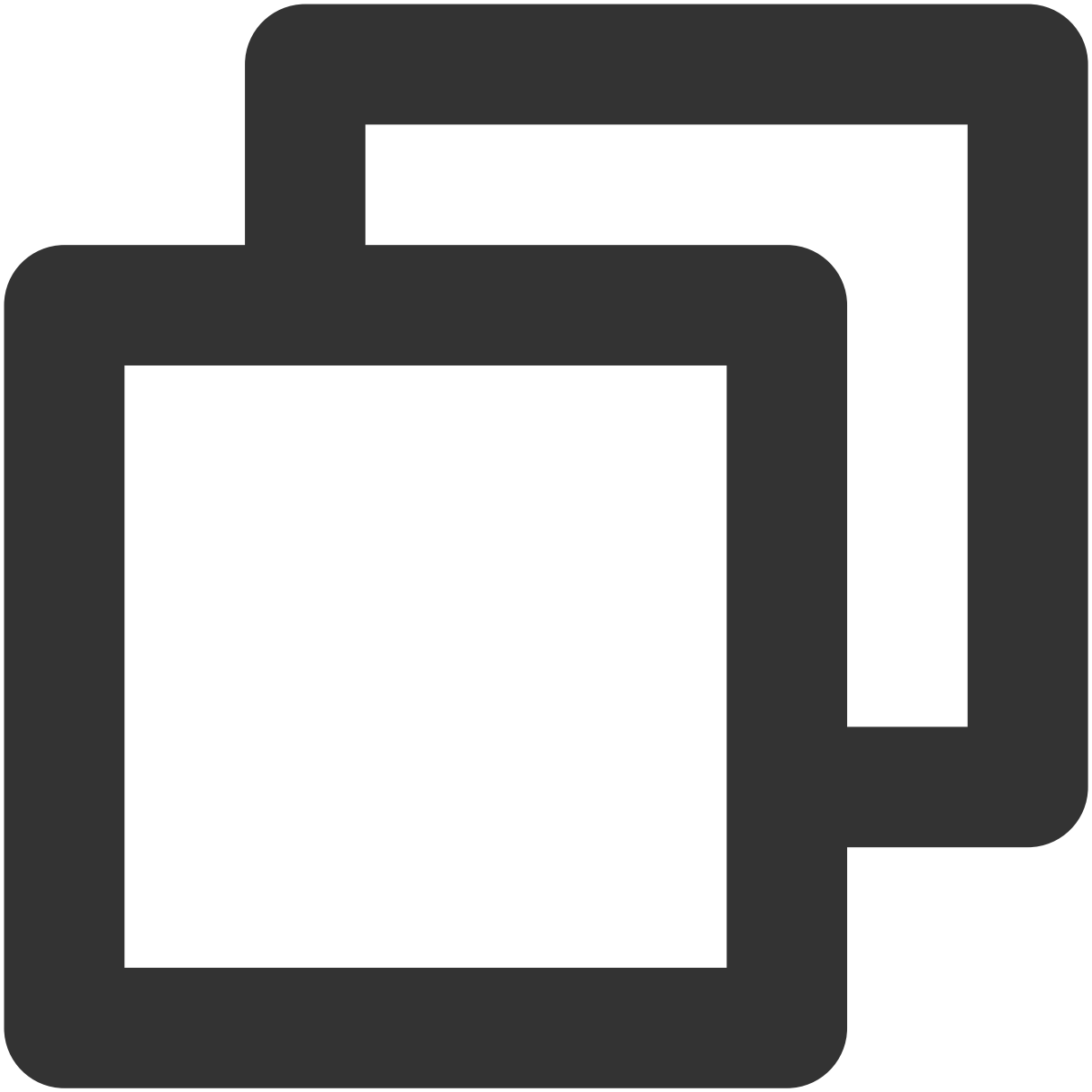
参数	数据类型	描述
access_token	String	OAuth 2.0 Access Token (JWT)。
token_type	String	Token 类型，目前取固定值 `Bearer` 。
expires_in	Number	Access Token 有效期，单位秒。
scope	String	Access Token 的 Scope。
refresh_token	String	OAuth 2.0 Refresh Token。
id_token	String	OIDC ID Token (JWT)。

说明：

CIAM 返回的是 JWT 格式的 ID Token，请参考 OIDC 官方文档 对 ID Token 进行解密验证。也可以直接使用相关的开发库完成解密验证。 验证所需的公钥通过调用 获取 JWT 公钥 接口获得。

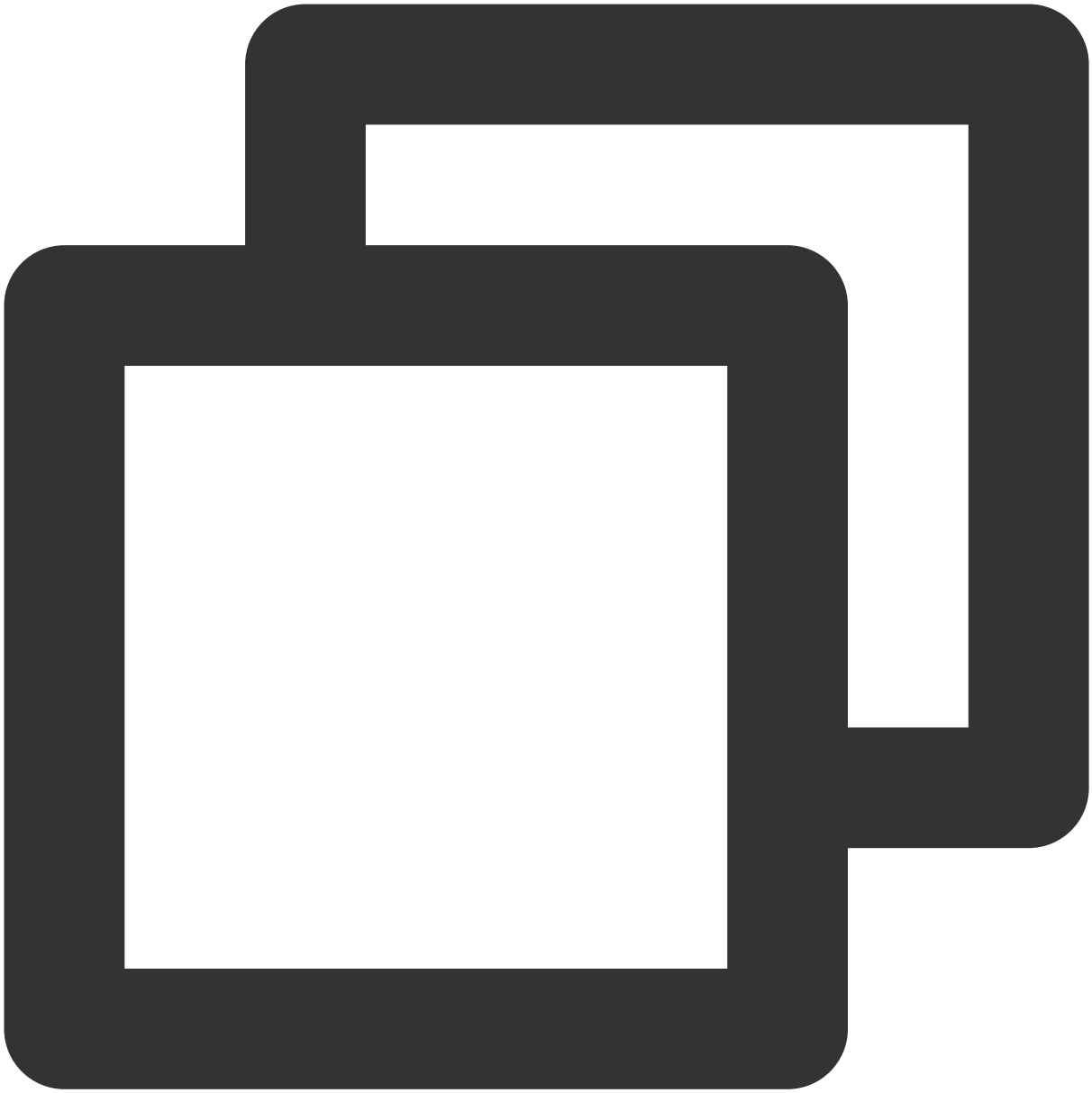
异常响应示例

client_id 参数缺失或有误。



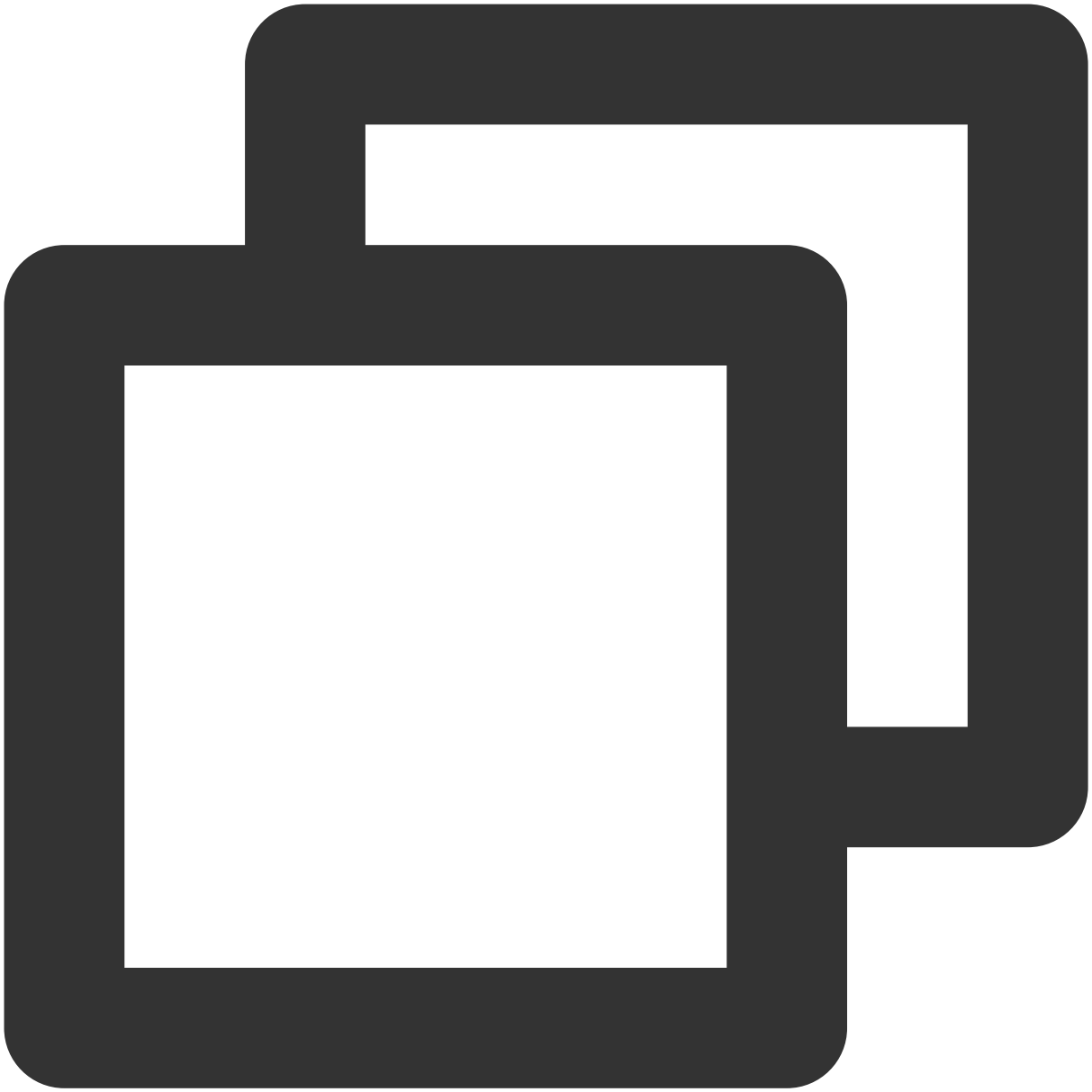
```
HTTP/1.1 401 Unauthorized
```

client_id 与获取授权和获取 Token 时使用的不一致。



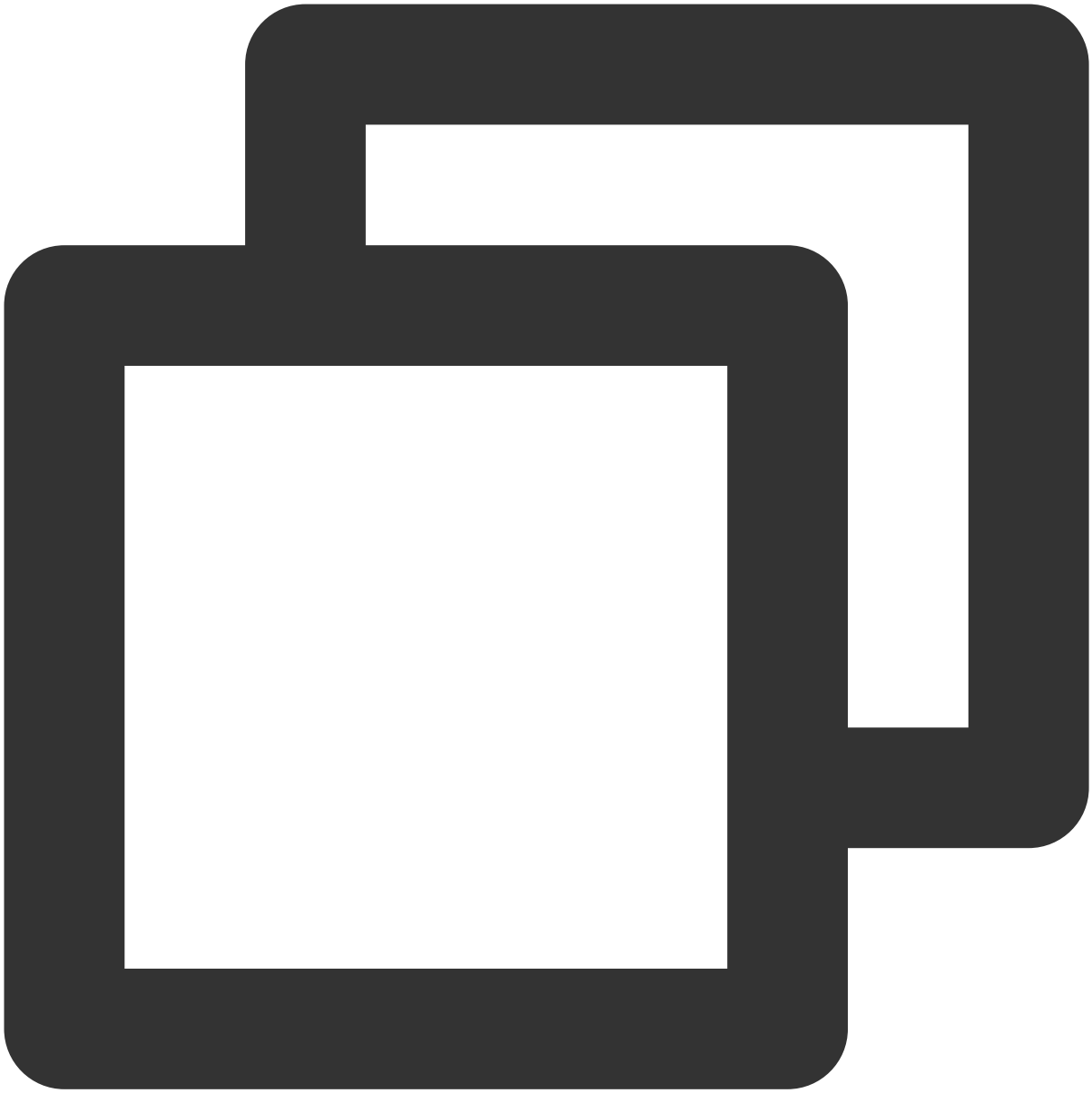
```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_client"
}
```

grant_type 参数有误。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "unsupported_grant_type",
"error_description" : "OAuth 2.0 Parameter: grant_type",
"error_uri" : "https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

code 参数有误。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_grant"
}
```

客户端凭证模式

最近更新时间：2023-12-22 11:42:08

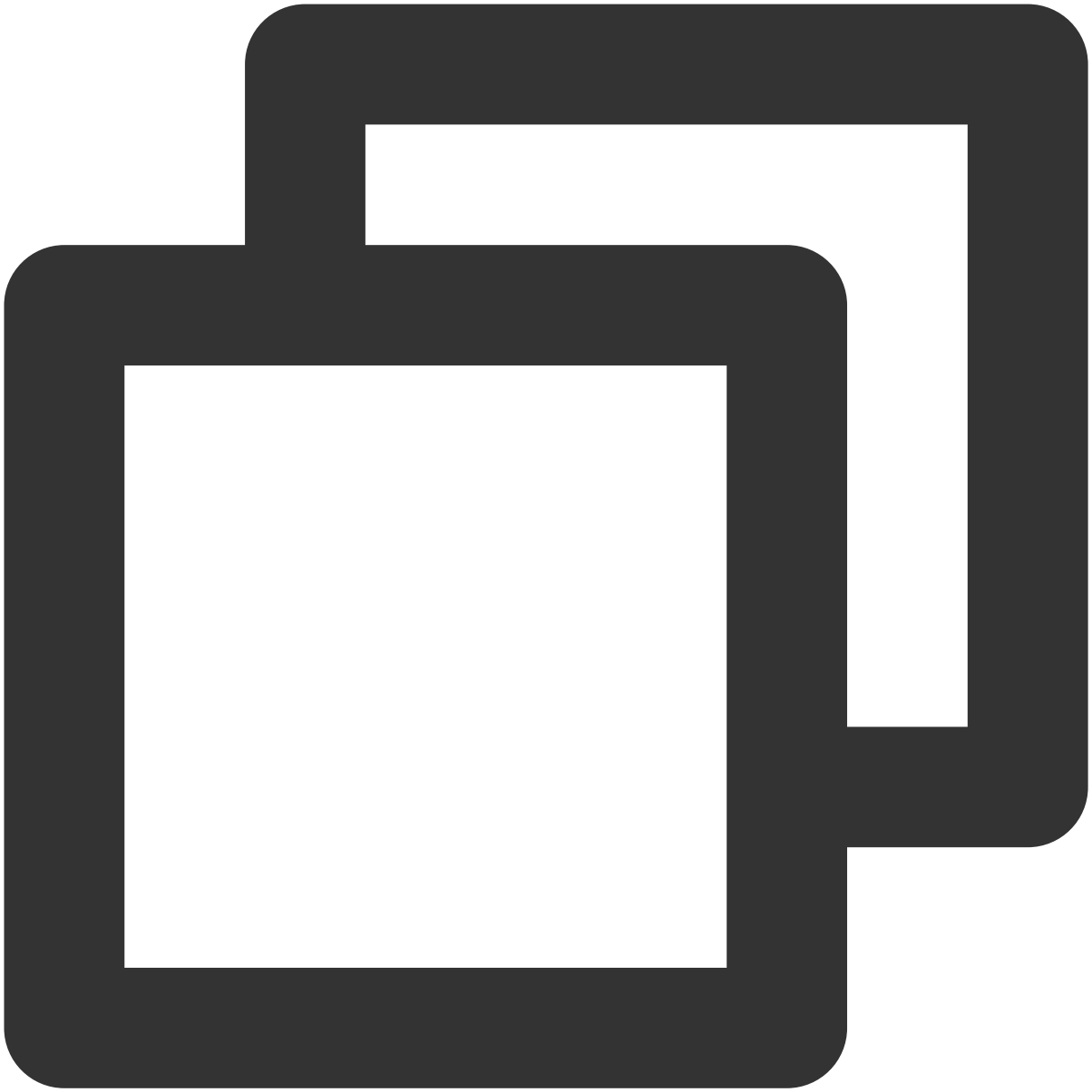
接口描述

使用 OAuth 客户端凭证模式 (client_credentials) 获取 Access Token 。

支持的应用类型

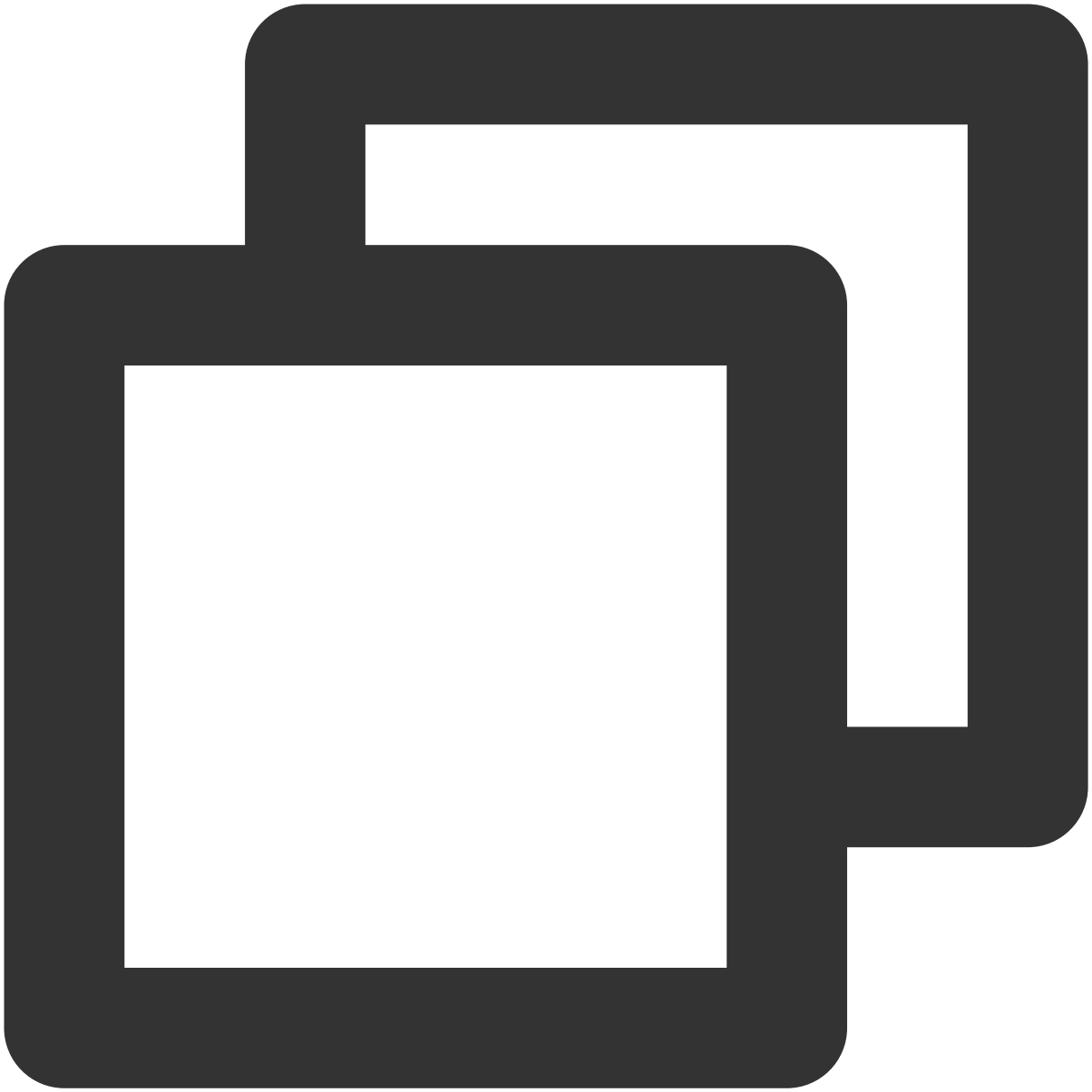
Web 应用、M2M 应用。

请求方法



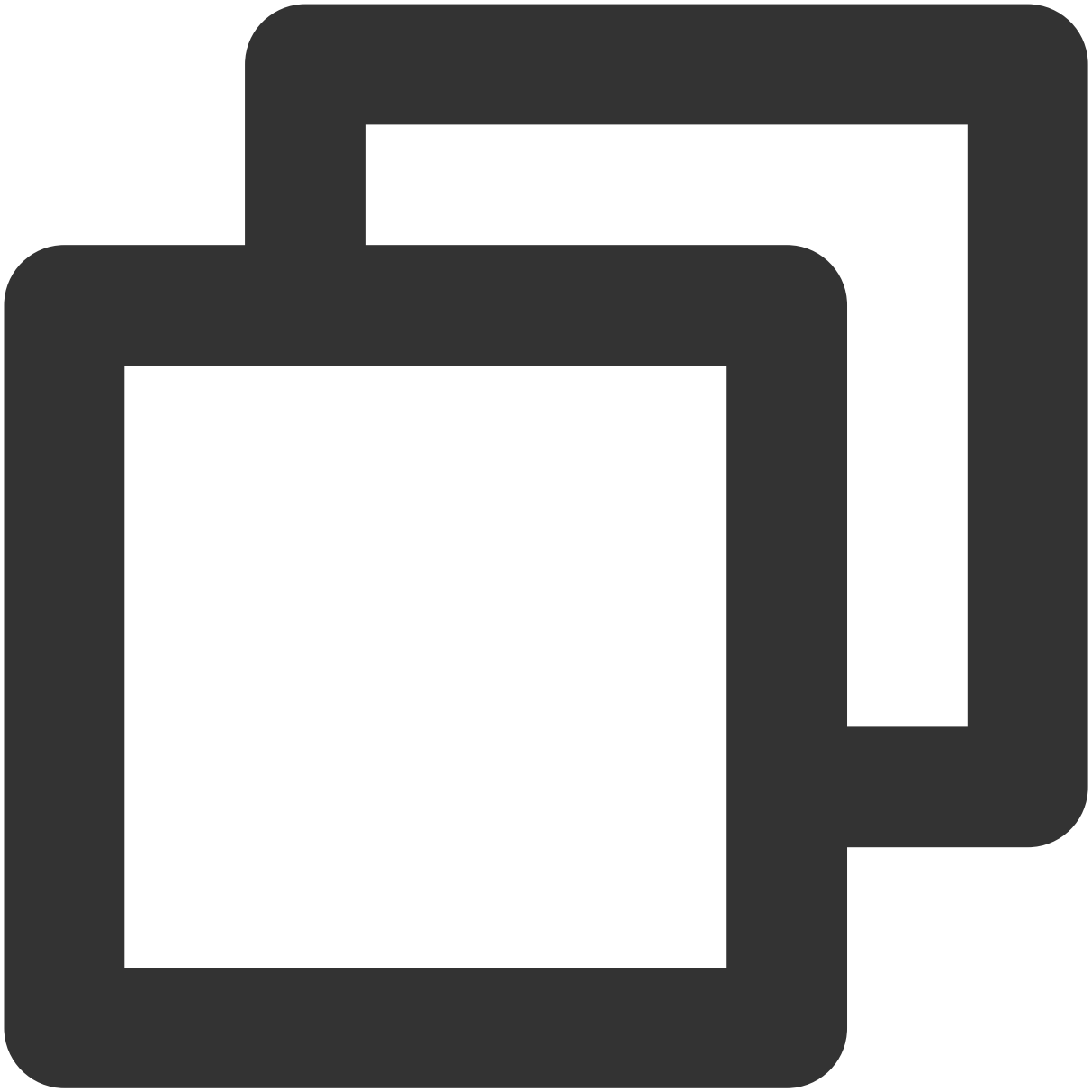
```
POST
```

请求路径



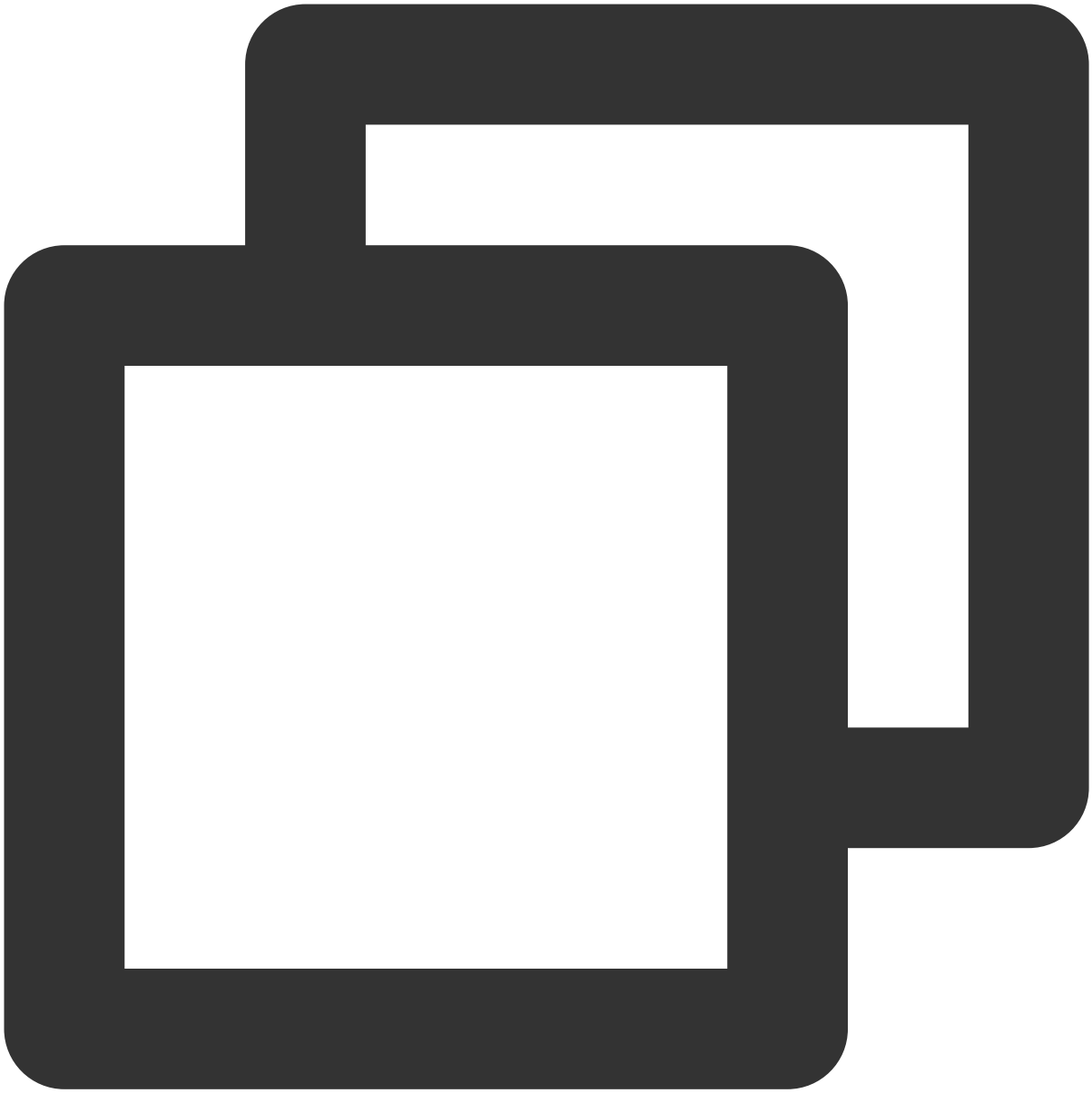
```
/oauth2/token
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例

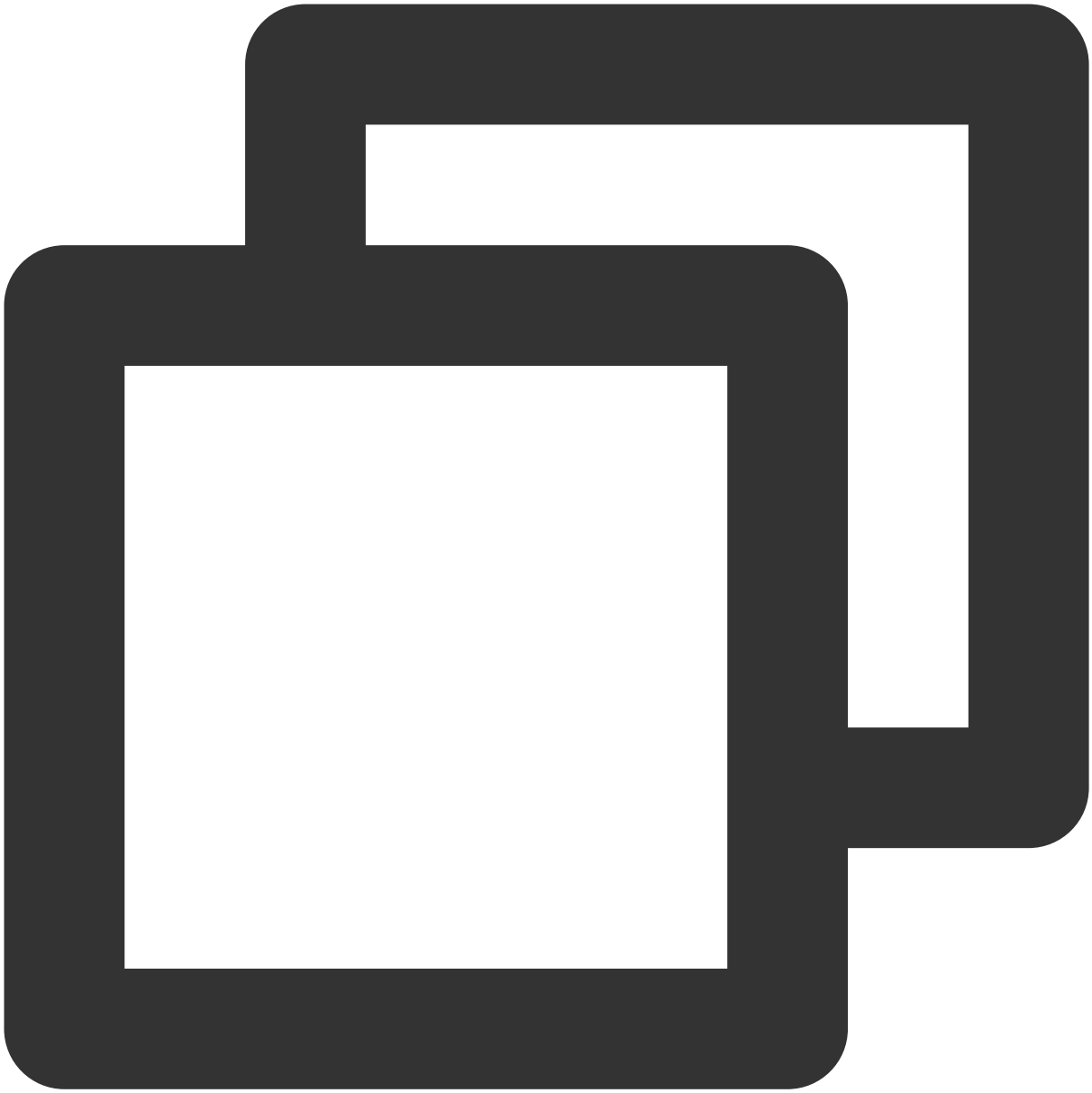


```
POST /oauth2/token HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_id=TENANT_CLIENT_ID&client_secret=TENANT_CLIEN
```

请求参数

参数	可选	描述
grant_type	false	填固定值 `client_credentials` 。
client_id	false	应用的 `client_id` 。可参考 应用管理页面 > **选定指定应用** > 单击**应用配置** > 对应的“Client Id”。
client_secret	false	应用的 `client_secret` 。可参考 应用管理页面 > **选定指定应用** > 单击**应用配置** > 对应的“client_secret”。
scope	true	申请授权的 `scope` ，多个 `scope` 之间使用空格分隔。

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiJmOTY5NGQ5My1kNTQxLTQ5ODUtODhkYy00MjIyOTg3MzAwOGUiLCJ
  "scope" : "identity_proofing",
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

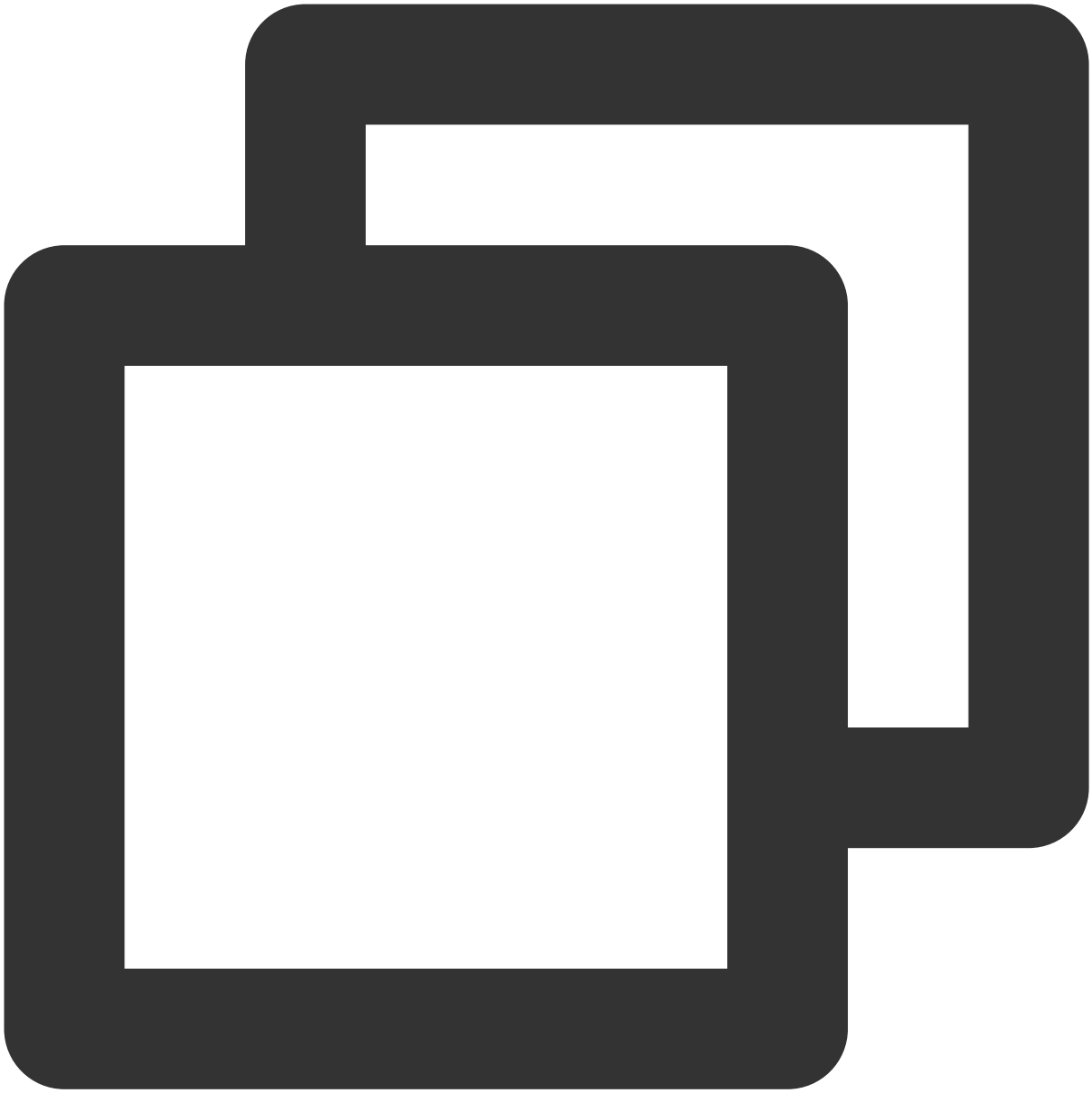
响应参数

参数	数据类型	描述
access_token	String	Access Token (JWT)。
token_type	String	Token 类型，目前返回的是固定值 `Bearer` 。
expires_in	Number	Access Token 有效期，单位秒。
scope	String	Access Token 的 Scope。

说明：
客户端凭证模式的响应中不包含 Refresh Token。当 Access Token 过期时，应用再次调用此接口获取新的 Access Token。

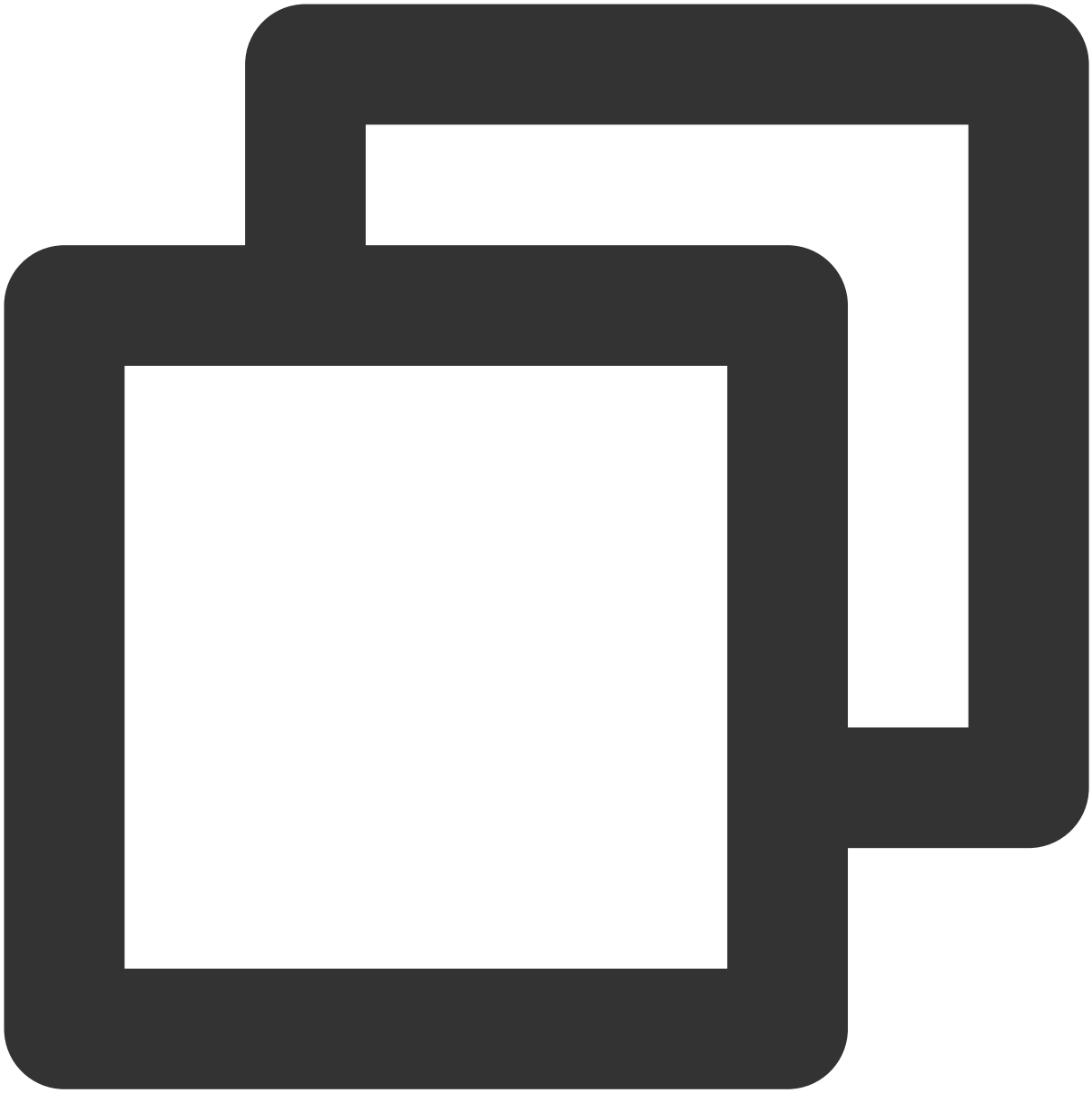
异常响应示例

应用不存在、未开启或应用密钥校验失败。



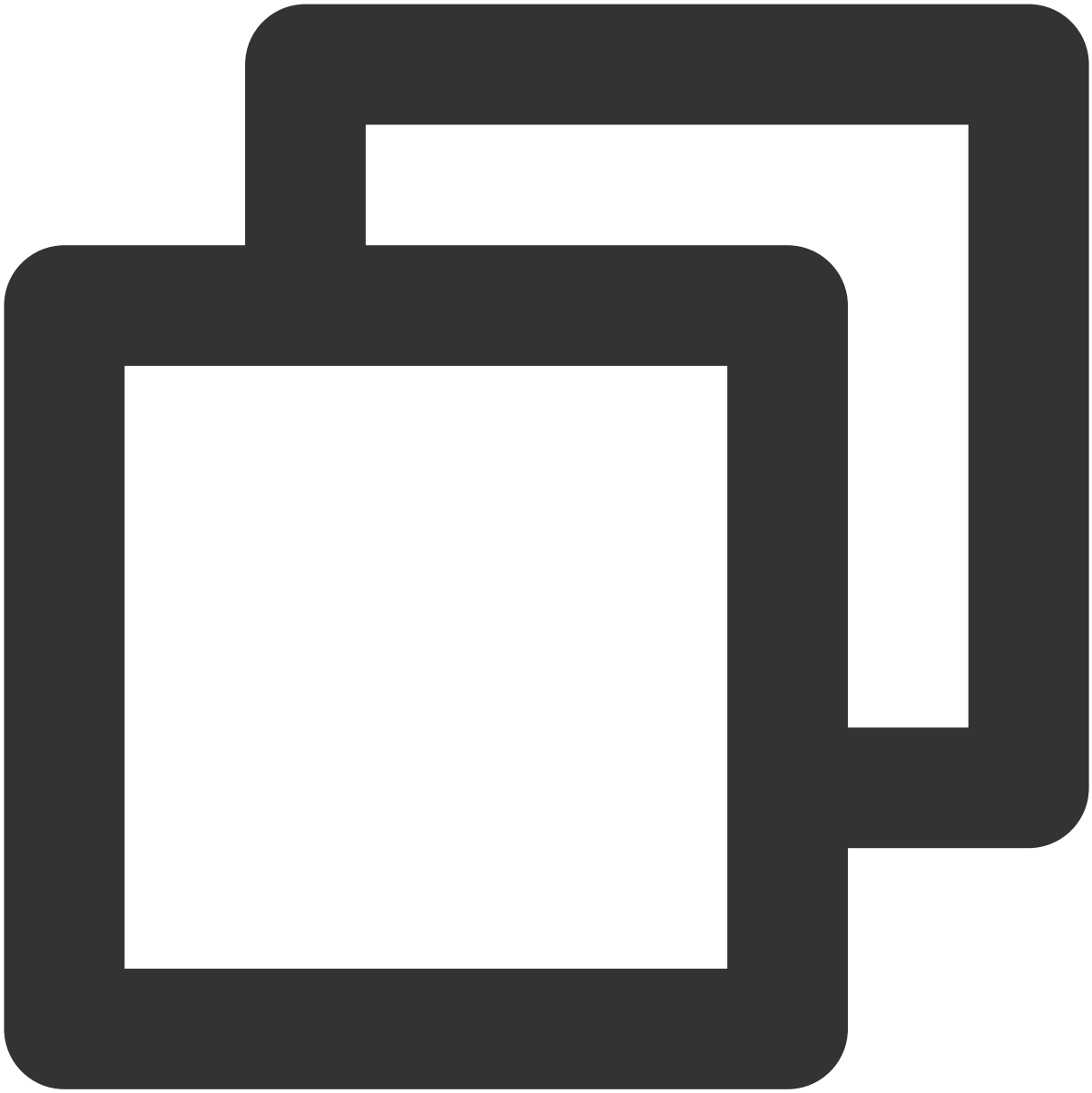
```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_client"
}
```

应用无权限使用 `client_credentials` 模式获取 Token。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "unauthorized_client"
}
```

scope 参数有误或超出应用权限。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
"error" : "invalid_scope"
}
```

获取 JWT 公钥

最近更新时间：2023-12-22 11:42:07

接口描述

JWT 公钥用于对 JWT 格式的 ID Token 和 Access Token 进行验证。

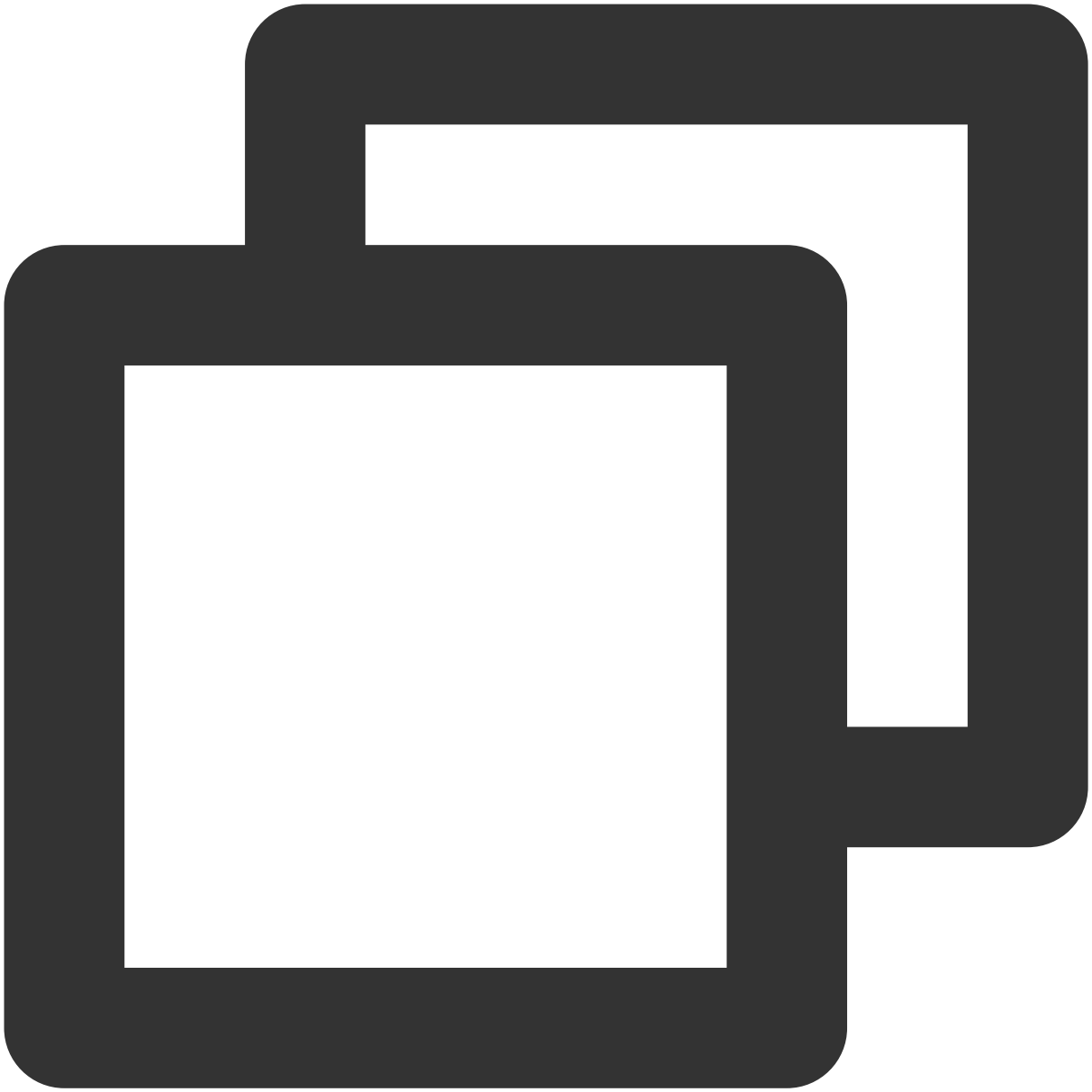
说明：

JWT 密钥在创建用户目录时自动生成，不同用户目录的密钥不同。

支持的应用类型

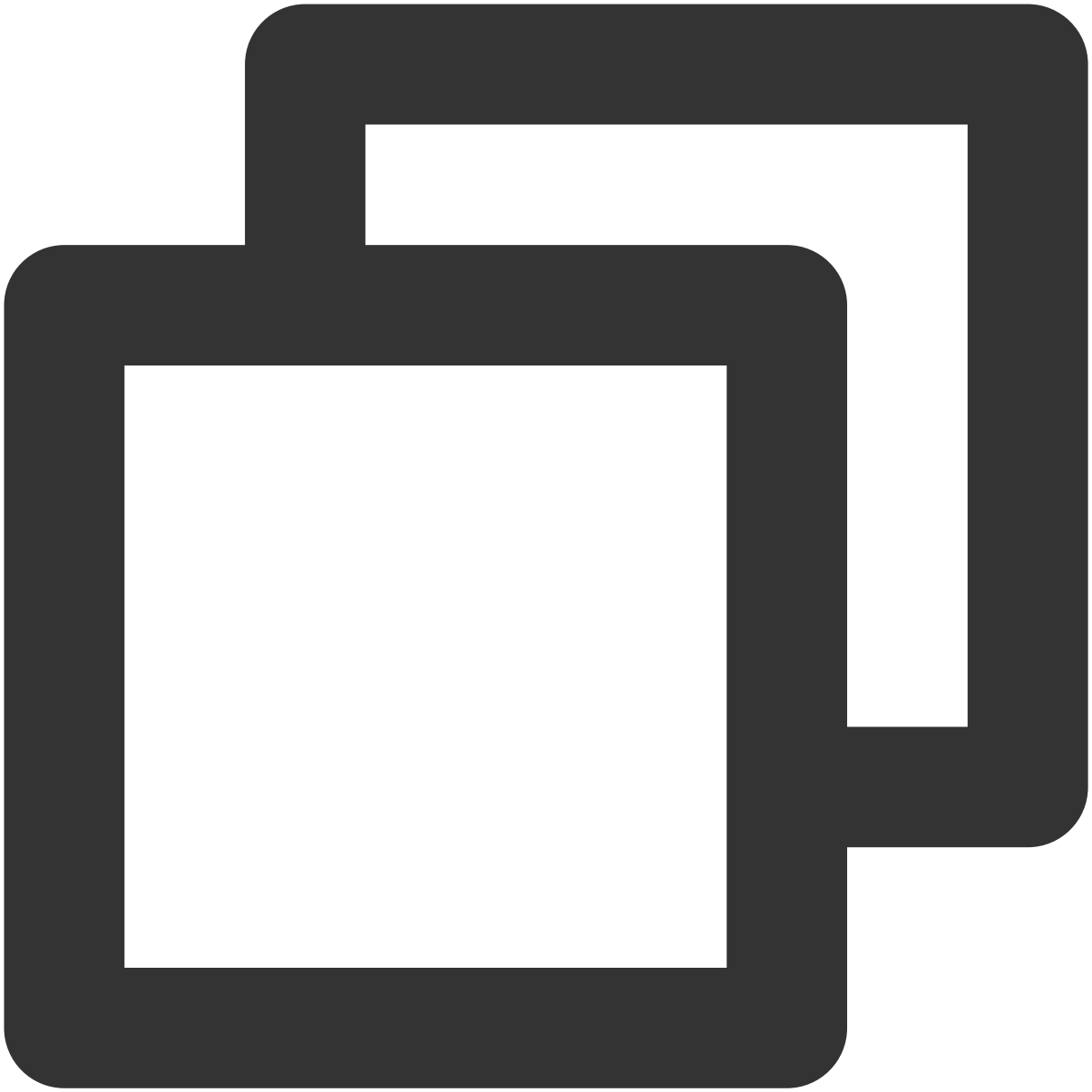
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



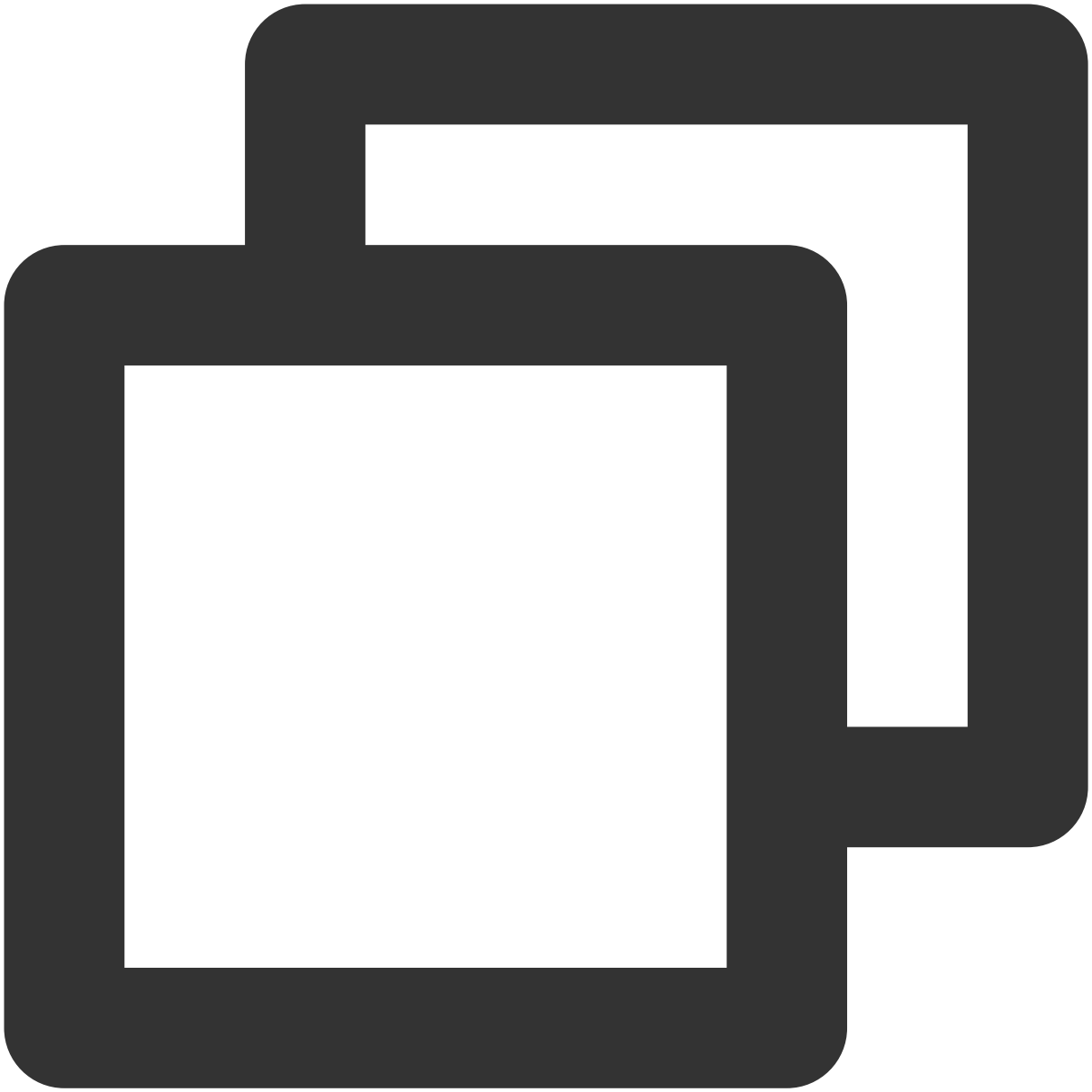
```
GET
```

请求路径



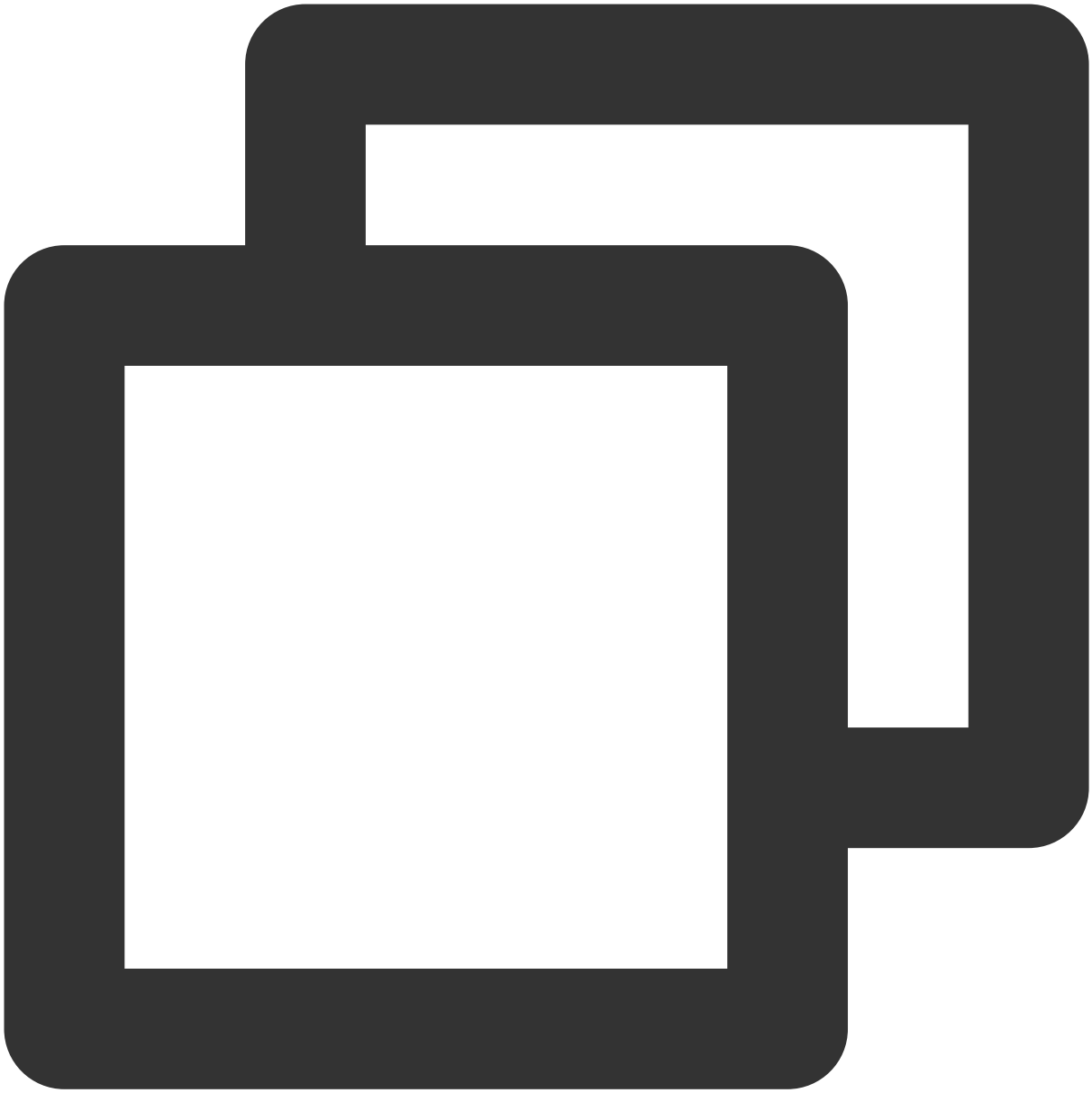
```
/oauth2/jwks
```

请求示例



```
GET /oauth2/jwks HTTP/1.1
Host: sample.portal.tencentciam.com
```

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "keys" : [ {
    "kty" : "RSA",
    "e" : "AQAB",
    "kid" : "f9694d93-d541-4985-88dc-42229873008e",
    "n" : "wYmf-IL7_pXqEjtfHme7KqS06hRQ0BzhTzORjgwnsJD_CPexMHQAd82vZfOQioW9oaMXTiSA
  } ]
}
```

响应参数

参数	数据类型	描述
keys	Array	包含公钥的数组。
keys[].kty	String	密钥类型，如 RSA。
keys[].kid	String	密钥标识。
keys[].e	String	RSA 公钥。
keys[].n	String	RSA 公钥。

刷新 Token

最近更新时间：2023-12-22 11:43:32

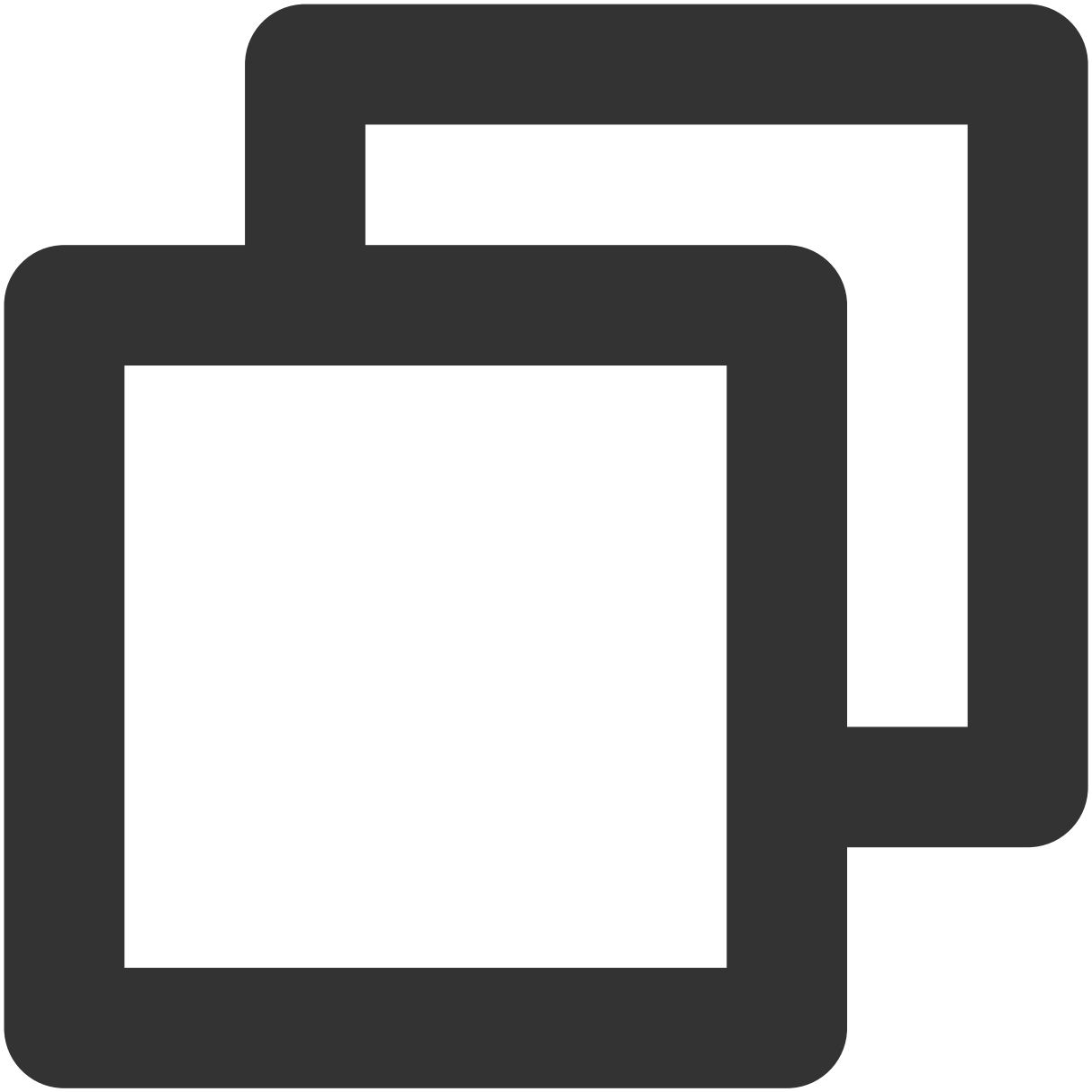
接口描述

使用 refresh_token 获取新的 access_token。

支持的应用类型

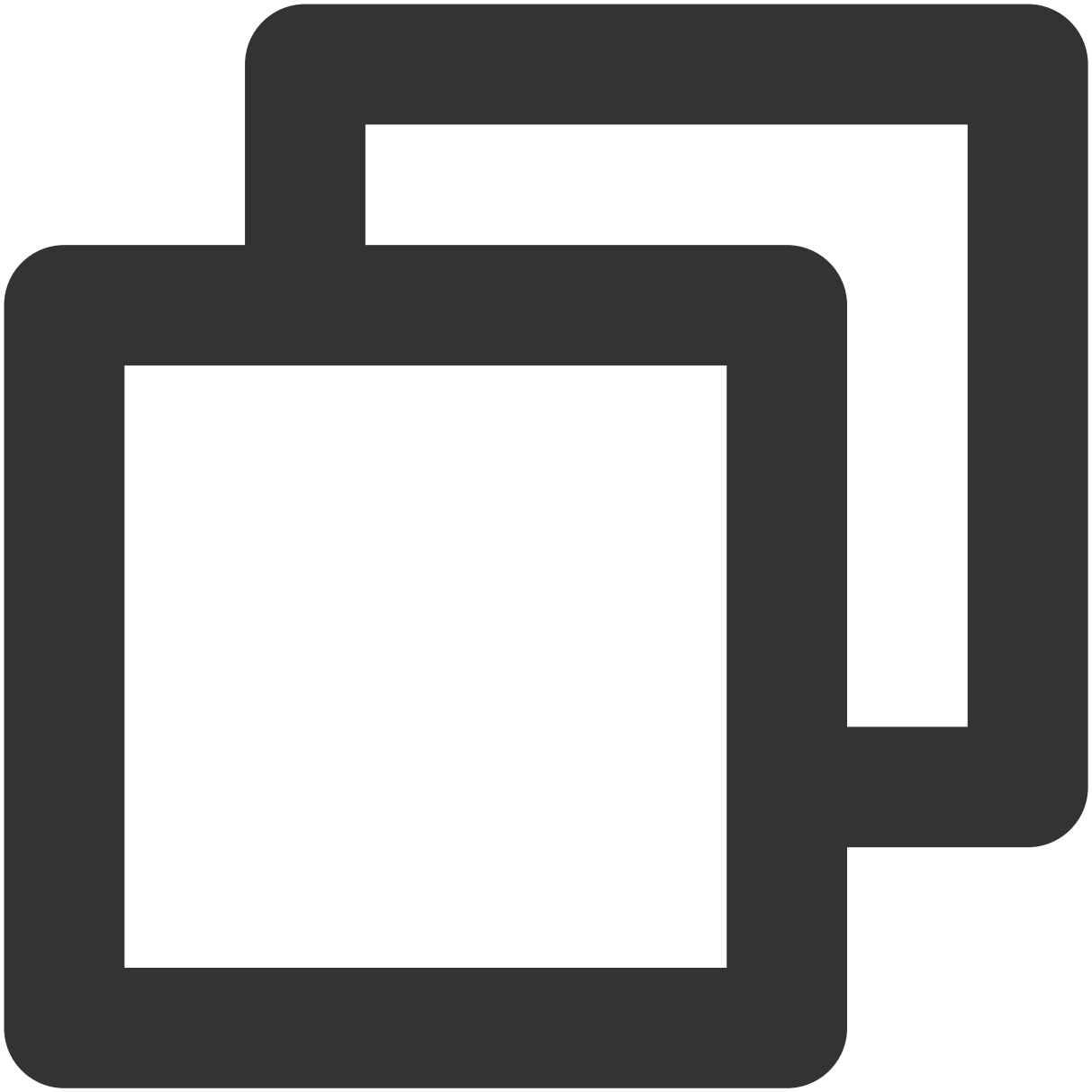
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



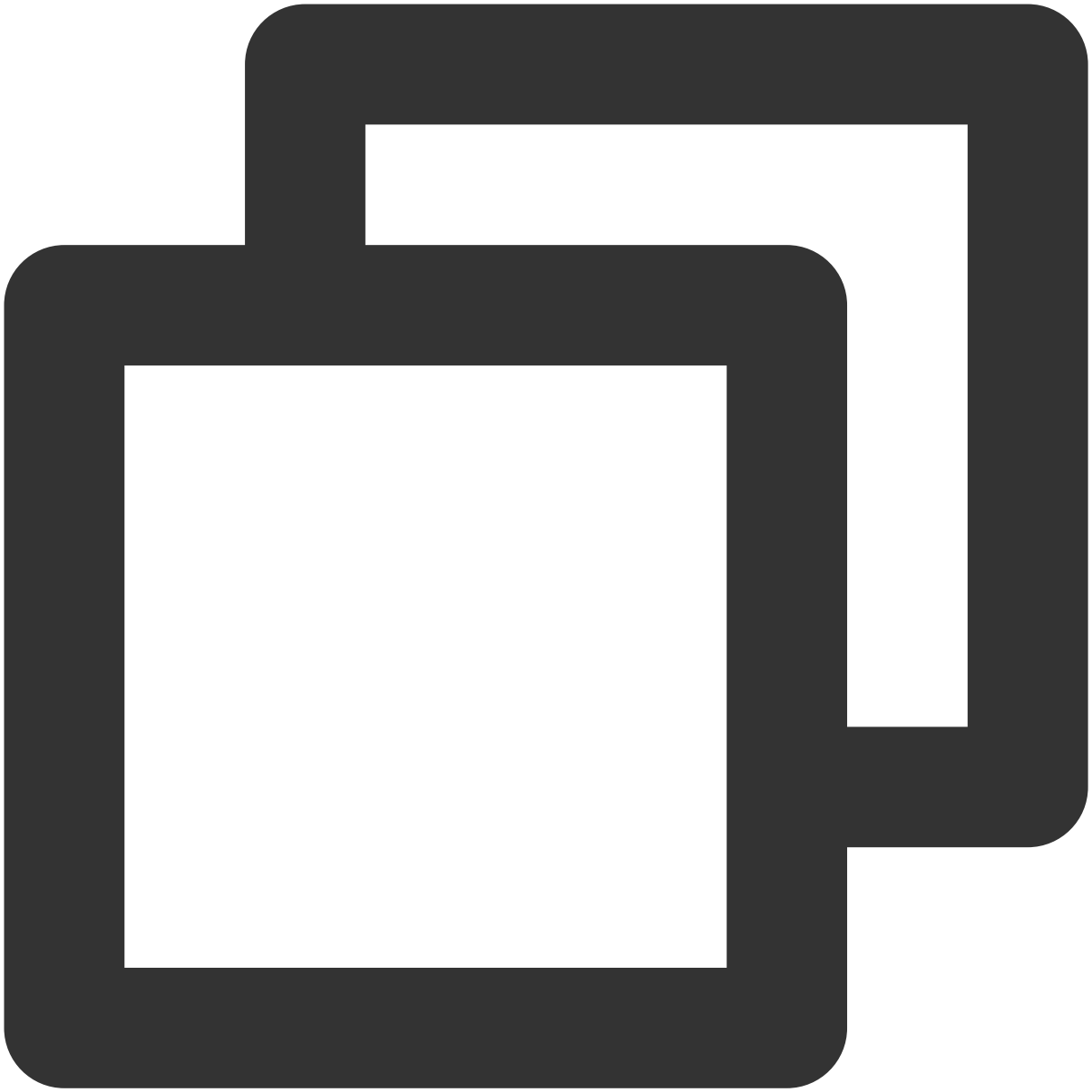
```
POST
```

请求路径



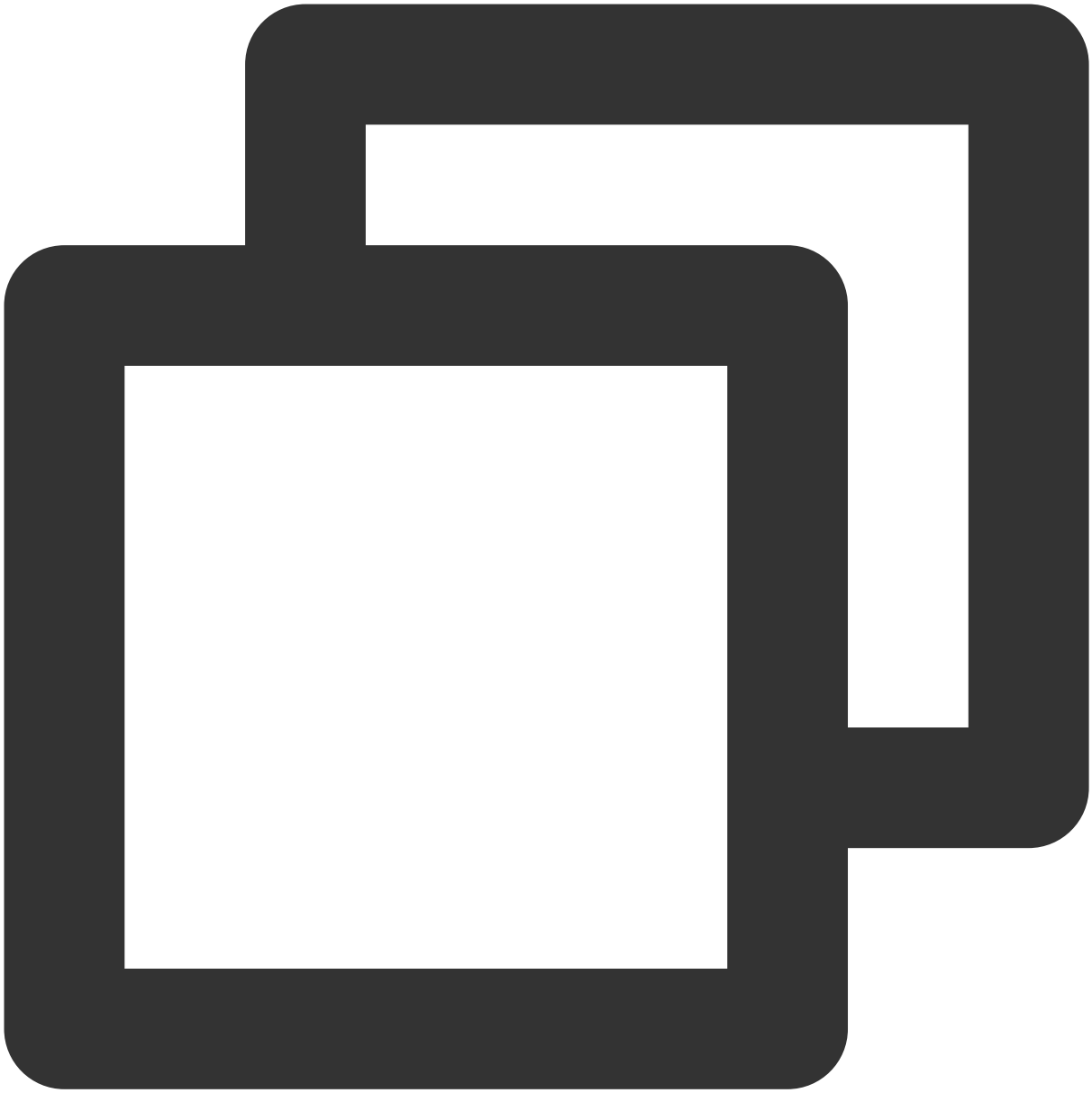
```
/oauth2/token
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例

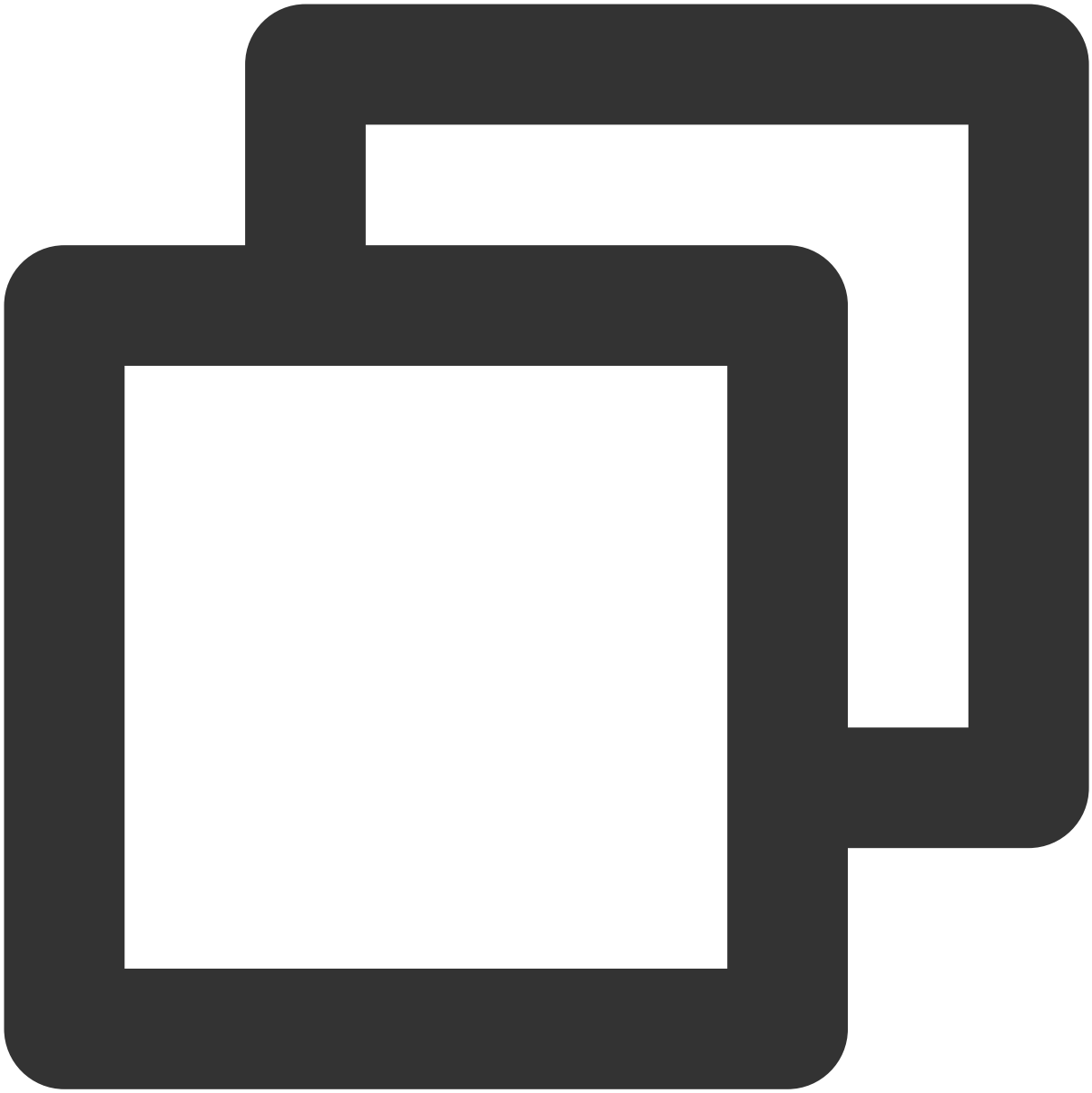


```
POST /oauth2/token HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded

client_id=TENANT_CLIENT_ID&client_secret=TENANT_CLIENT_SECRET&grant_type=refresh_to
```

请求参数

参数	可选	描述
client_id	false	应用的 `client_id` 。需要与获取授权时使用的一致。
client_secret	false	应用的 `client_secret` 。可通过租户管理平台的应用基本信息页面查看。
grant_type	false	填固定值 `refresh_token` 。
refresh_token	false	获取 Token 时返回的 `refresh_token` 。

正常响应示例



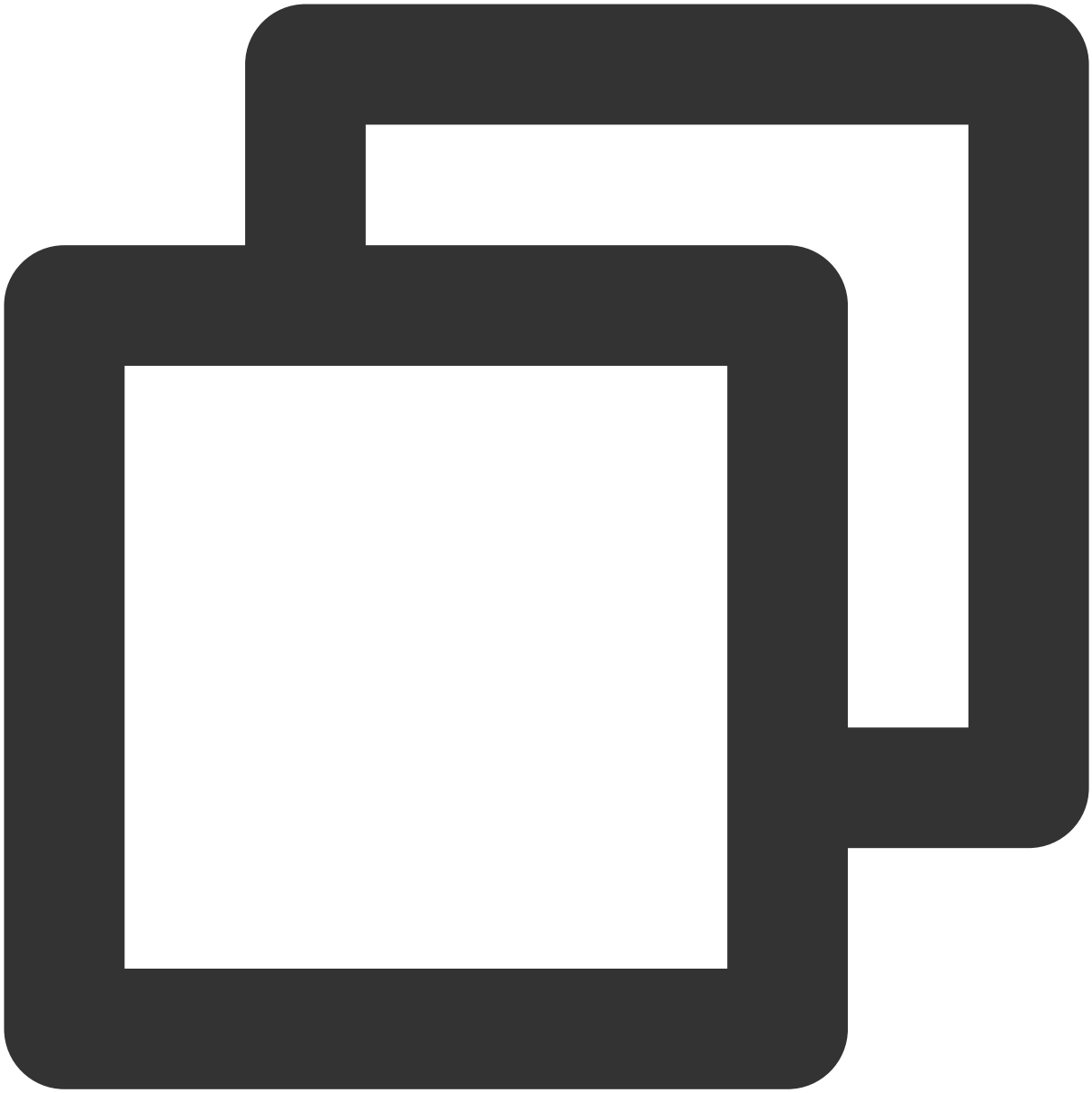
```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ
  "refresh_token" : "MOCK_REFRESH_TOKEN",
  "scope" : "openid",
  "id_token" : "eyJraWQiOiJkNDliYzUwNS01NTcyLTRlZDYtOWU0OC0zODhjM2Q0NGJiNDYiLCJ0eXA
  "token_type" : "Bearer",
  "expires_in" : 299
}
```

响应参数

参数	数据类型	描述
access_token	String	刷新后的 OAuth 2.0 Access Token (JWT)。
refresh_token	String	刷新后的 OAuth 2.0 Refresh Token。
scope	String	Access Token 的 Scope。
id_token	String	刷新后的 OIDC ID Token (JWT)。
token_type	String	Token 类型，目前取固定值 `Bearer` 。
expires_in	Number	Access Token 有效期，单位秒。

异常响应示例

refresh_token 参数有误。



```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8

{
  "error" : "invalid_grant"
}
```

注销 Token

最近更新时间：2023-12-22 11:43:32

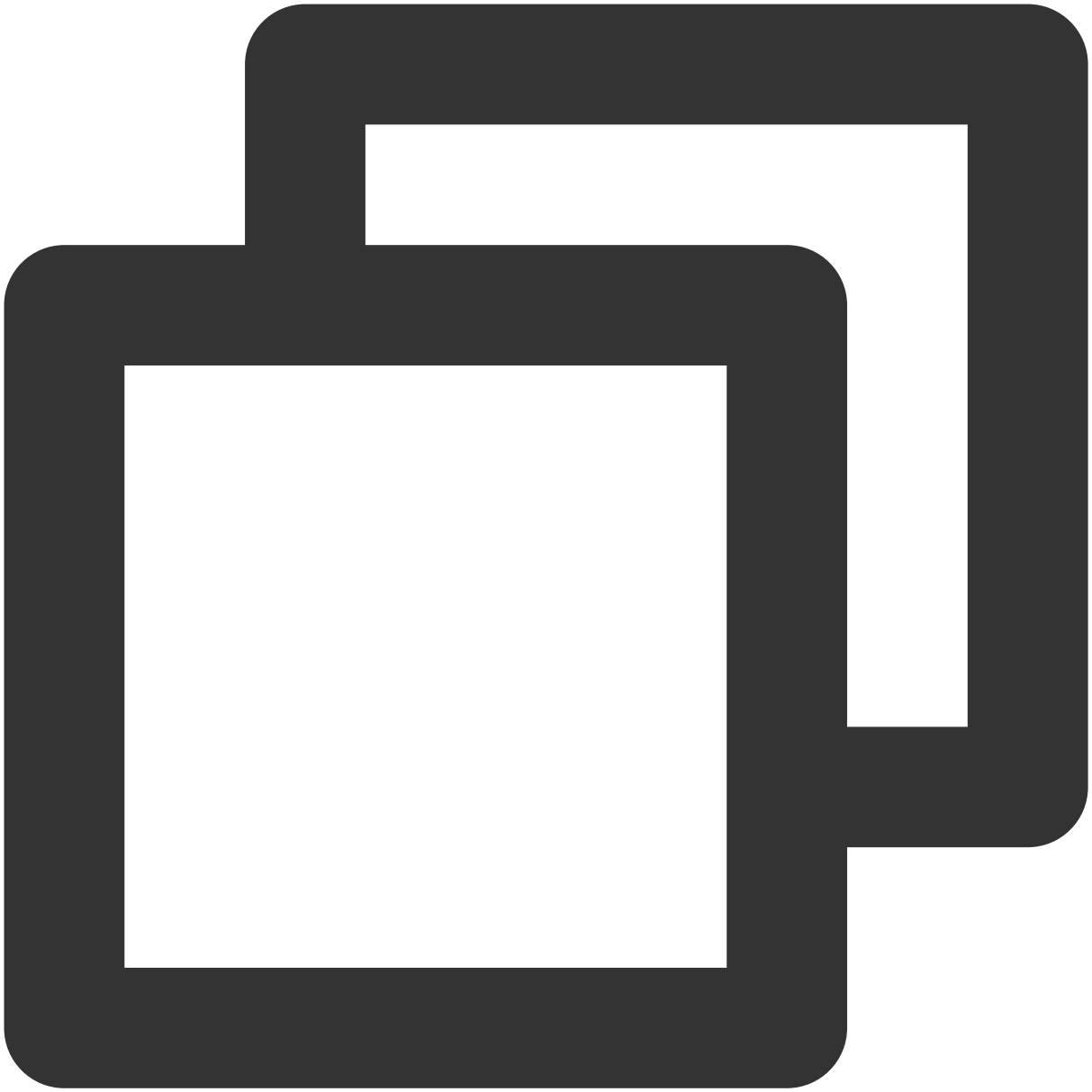
接口描述

注销 OAuth 2.0 Token 。如果传入的是 access_token ， 则仅注销该 access_token ；如果传入的是 refresh_token, 则该 refresh_token 以及与它相关联的 access_token 都将被注销。

支持的应用类型

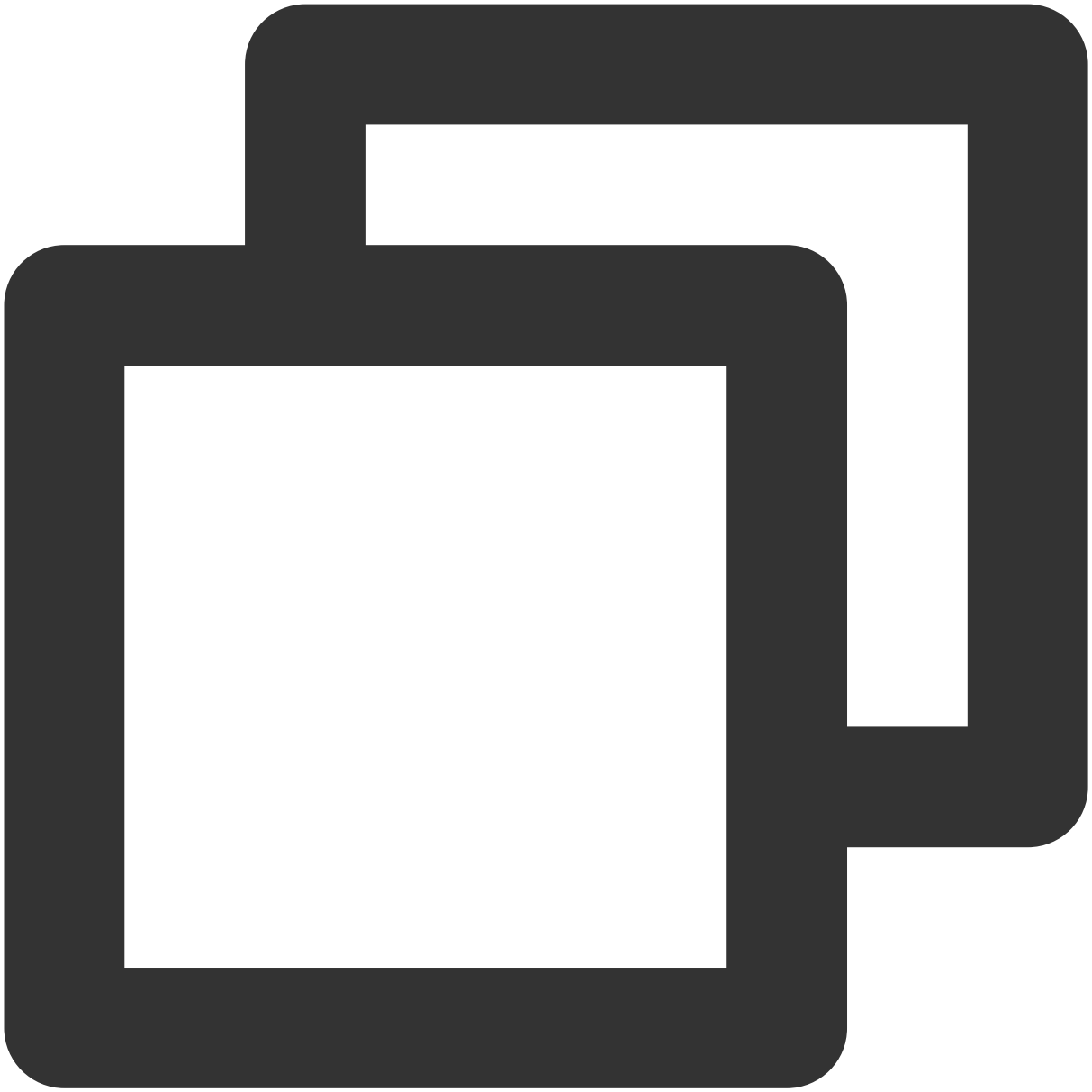
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



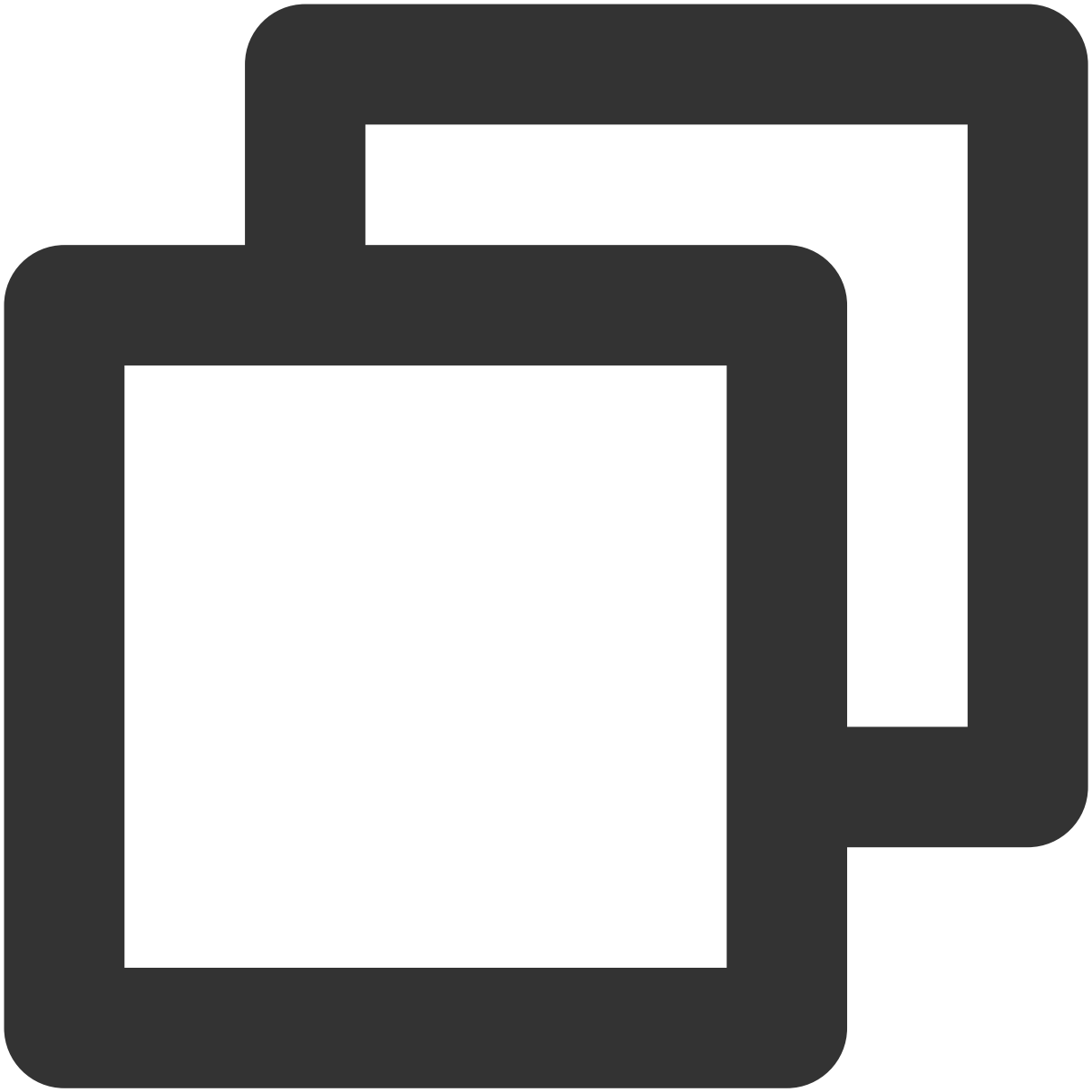
```
POST
```

请求路径



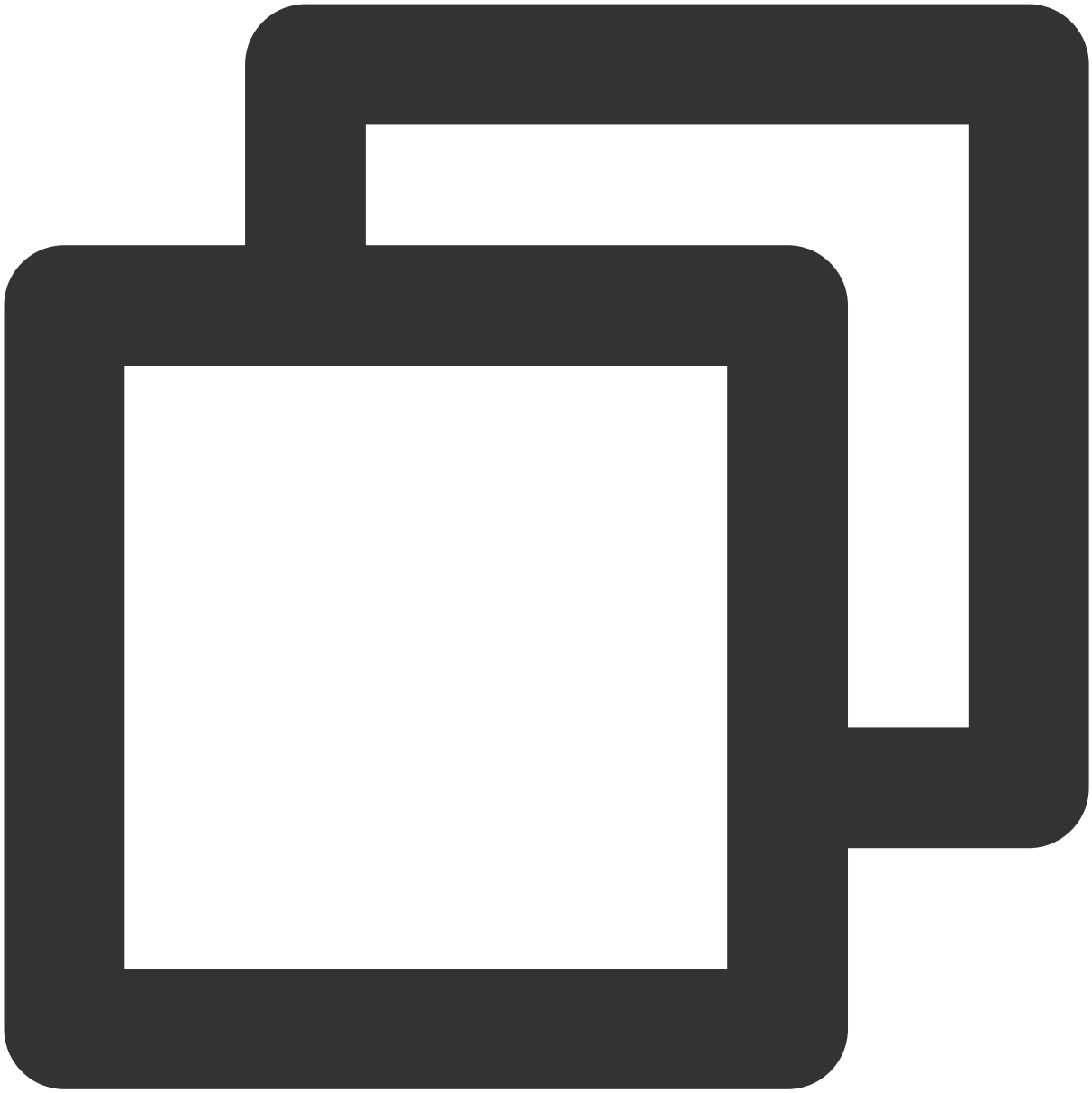
```
/oauth2/revoke
```

请求 Content-Type



```
application/x-www-form-urlencoded
```

请求示例

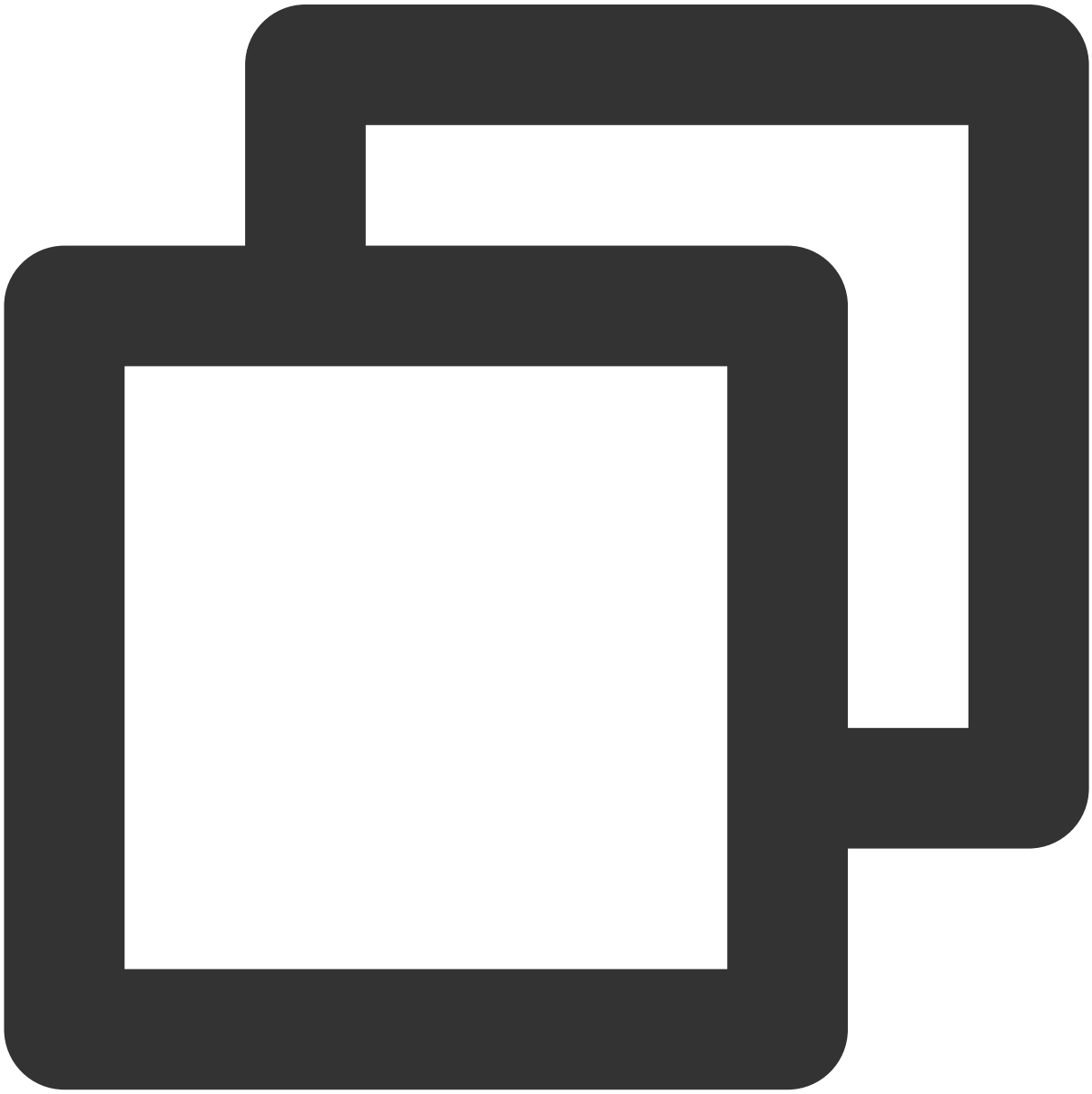


```
POST /oauth2/revoke HTTP/1.1
Host: sample.portal.tencentciam.com
Content-Type: application/x-www-form-urlencoded

client_id=TENANT_CLIENT_ID&client_secret=TENANT_CLIENT_SECRET&token=MOCK_ACCESS_TOK
```

请求参数

参数	可选	描述
client_id	false	应用的 `client_id` 。需要与获取授权和获取 Token 时使用的一致。
client_secret	false	应用的 `client_secret` 。可通过租户管理平台的应用基本信息页面查看。
token	false	access_token 或 refresh_token 的值。

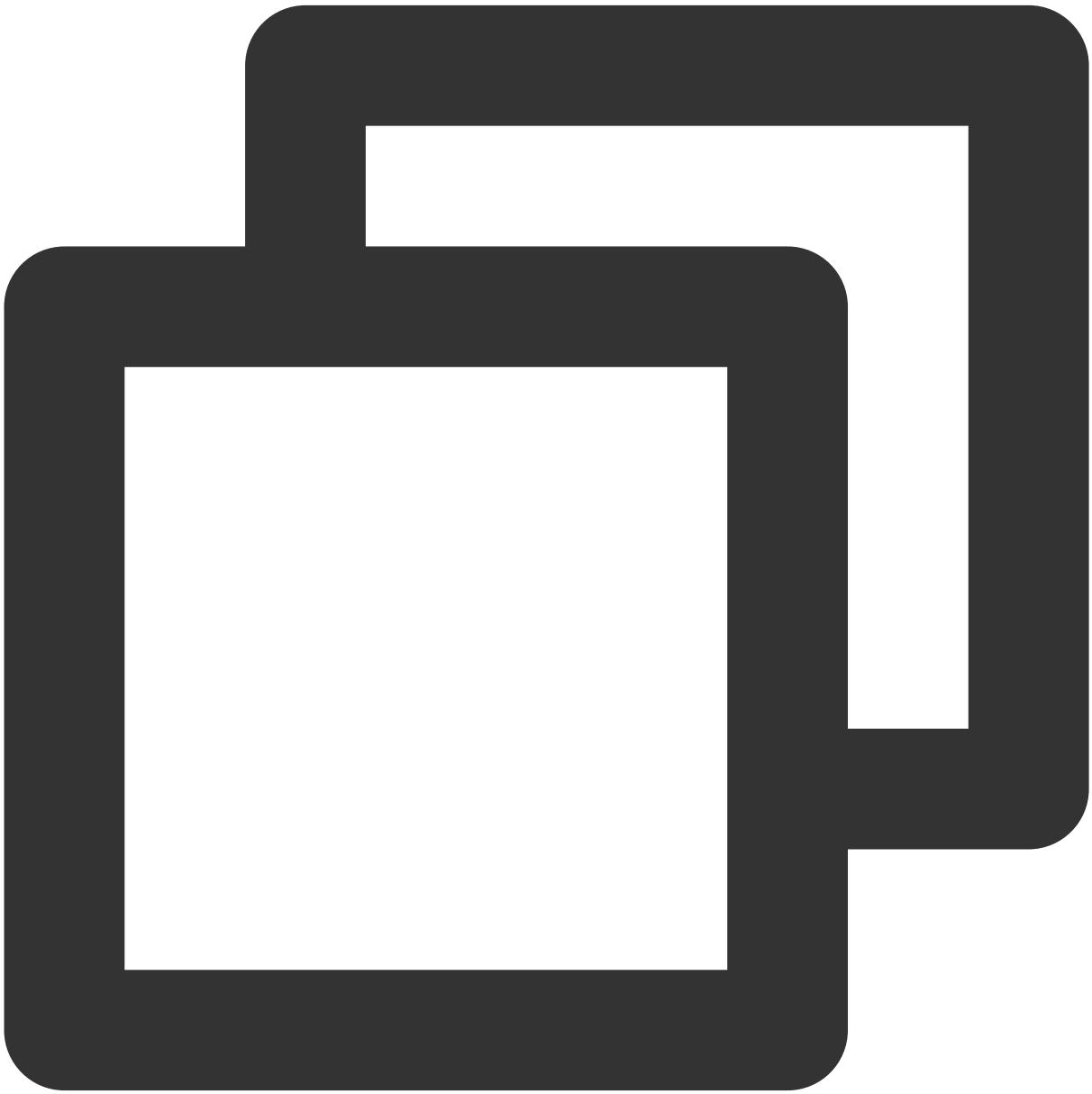
正常响应示例



```
HTTP/1.1 200 OK
```

异常响应示例

client_id 与发起登录和获取 Token 时使用的不一致。



```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8
```

```
{
  "error" : "invalid_client"
}
```

获取 OpenID Provider 配置信息

最近更新时间：2023-12-22 11:43:32

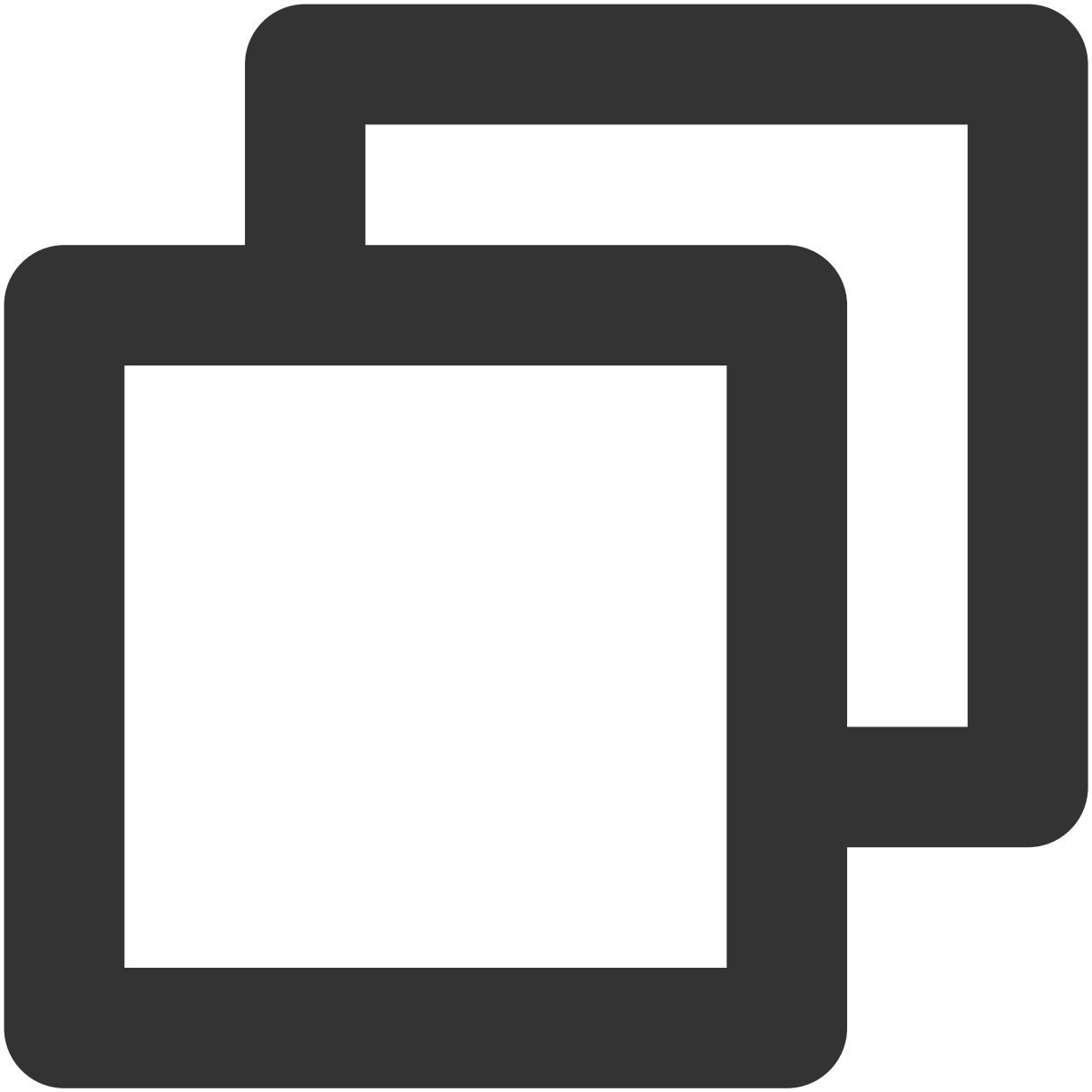
接口描述

应用可以通过此接口获取 OIDC 授权服务器的配置信息，从而简化本地配置。具体的配置信息及其含义请参考 OpenID Connect Discovery 标准。

支持的应用类型

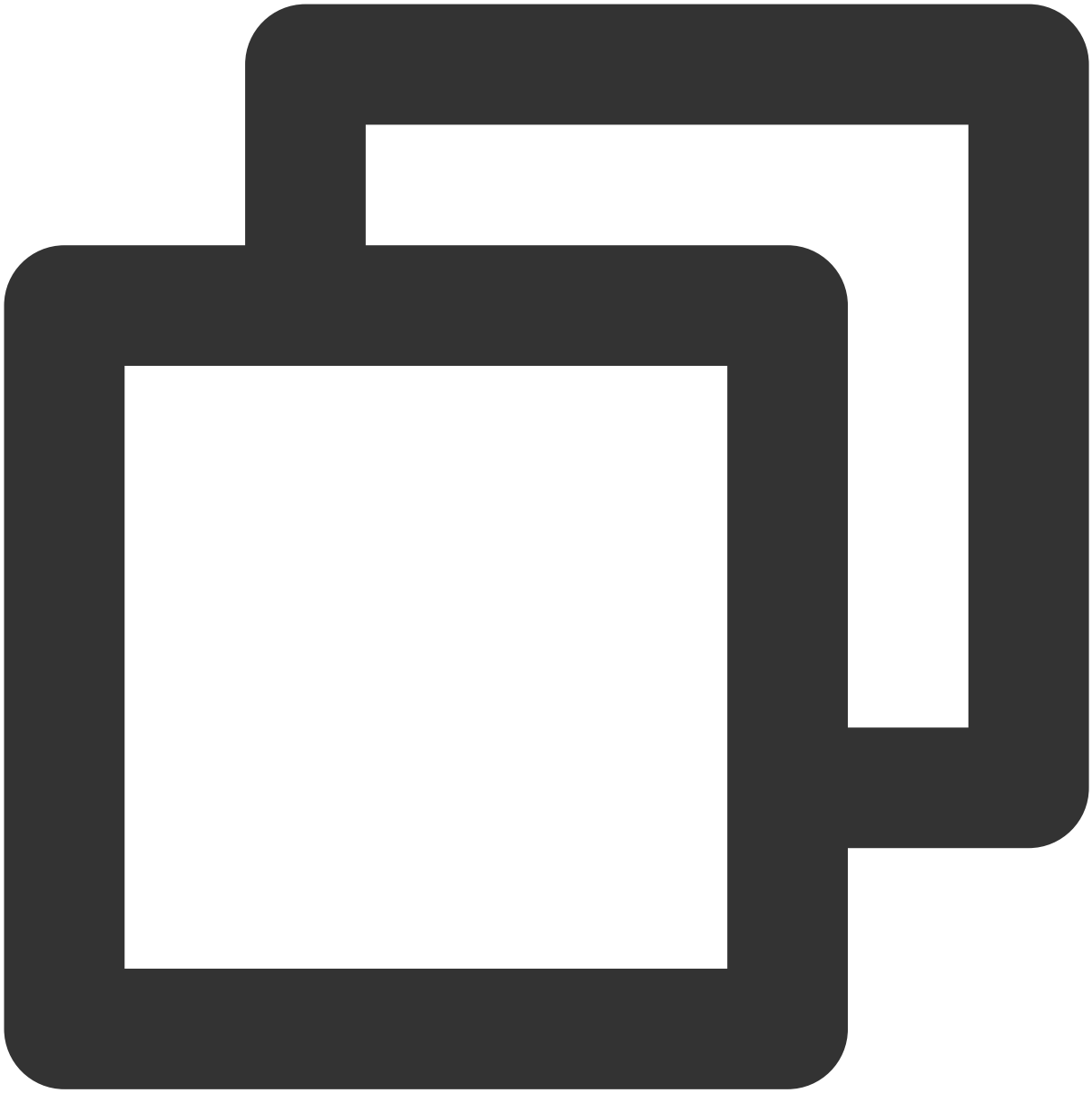
Web 应用、单页应用、移动 App、M2M 应用。

请求方法



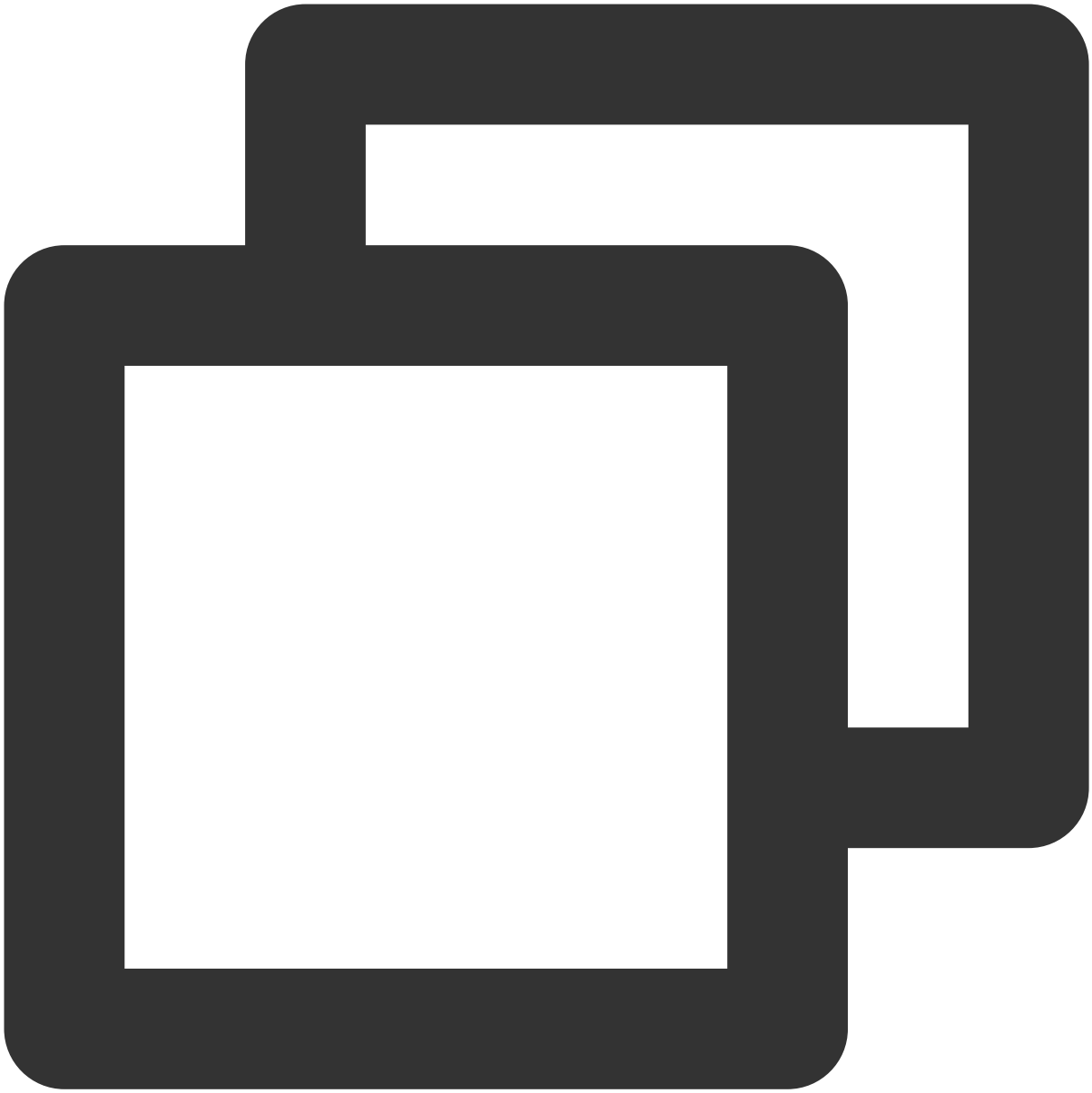
```
GET
```

请求路径



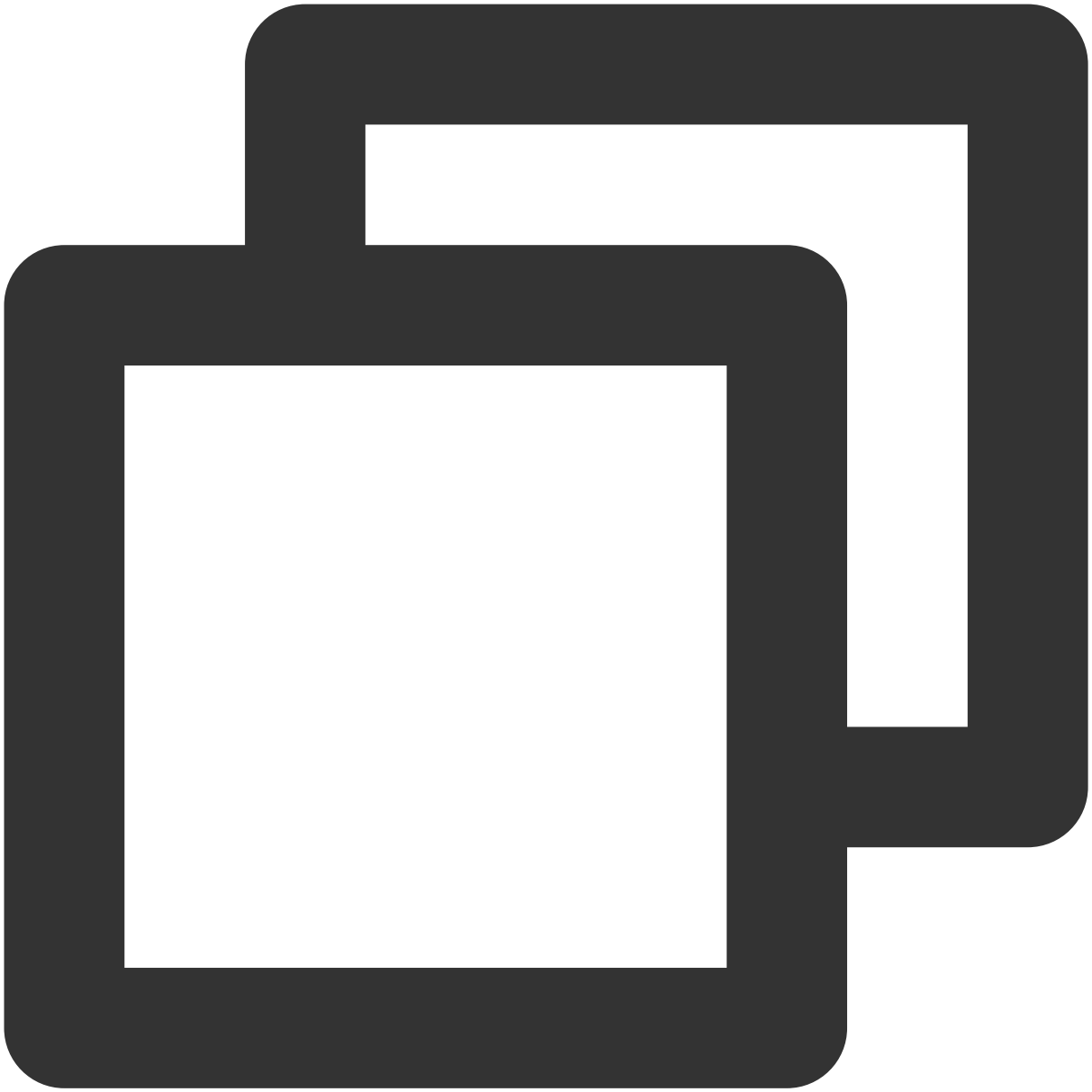
```
/.well-known/openid-configuration
```

请求示例



```
GET /.well-known/openid-configuration HTTP/1.1
Host: sample.portal.tencentciam.com
```

正常响应示例



```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "issuer" : "https://sample.portal.tencentciam.com",
  "authorization_endpoint" : "https://sample.portal.tencentciam.com/oauth2/authoriz
  "token_endpoint" : "https://sample.portal.tencentciam.com/oauth2/token",
  "token_endpoint_auth_methods_supported" : [ "client_secret_basic", "client_secret
  "jwks_uri" : "https://sample.portal.tencentciam.com/oauth2/jwks",
  "response_types_supported" : [ "code" ],
  "grant_types_supported" : [ "authorization_code", "client_credentials", "refresh_
```

```
  "subject_types_supported" : [ "public" ],
  "id_token_signing_alg_values_supported" : [ "RS256" ],
  "scopes_supported" : [ "openid" ]
}
```

响应参数

参数	数据类型	描述
issuer	String	OIDC Issuer。
authorization_endpoint	String	OAuth 2.0 获取授权的服务地址。
token_endpoint	String	OAuth 2.0 获取 Token 的服务地址。
jwks_uri	String	获取 JWT 公钥的服务地址。
grant_types_supported	Array	支持的 OAuth 2.0 Grant Type。
response_types_supported	Array	OAuth 2.0 获取授权服务支持的 Response Type。
token_endpoint_auth_methods_supported	Array	OAuth 2.0 获取 Token 服务支持的认证方式。
subject_types_supported	Array	支持的 OIDC Subject Identifier Type。
id_token_signing_alg_values_supported	Array	支持的 JWS 签名算法。
scopes_supported	Array	支持的 OAuth 2.0 Scope。